Lucas Vinícius de Oliveira
Ricardo Orige de Bem

ANÁLISE E PROPOSTA DE MELHORIA NA ESTRUTURA DE REDES SEM FIO EM ESCOLAS PÚBLICAS NA MICRORREGIÃO DE ARARANGUÁ

Trabalho de Conclusão de Curso apresentado ao Curso de Tecnologias da Informação e Comunicação, do Campus Araranguá, da Universidade Federal de Santa Catarina, como requisito parcial para obtenção do título de Bacharel em Tecnologias da Informação e Comunicação.

Orientador: Prof. Dr. Juarez Bento da Silva,

Coorientador: Prof. Dr. Paulo Manoel Mafra

Araranguá

2017

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Oliveira, Lucas Vinicius de
ANÁLISE E PROPOSTA DE MELHORIA NA ESTRUTURA DE REDES SEM FIO EM ESCOLAS PÚBLICAS NA MICRORREGIÃO DE ARARANGUÁ / Lucas Vinicius de Oliveira ; orientador, Juarez Bento da Silva, coorientador, Paulo Manoel Mafra, 2017.
81 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2017.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Redes sem fio. 3. Experimentação Remota. 4. Ensino Básico. 5. Tecnologias na Educação. I. Silva, Juarez Bento da. II. Mafra, Paulo Manoel. III. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. IV. Título.

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Bem, Ricardo Orige de
ANÁLISE E PROPOSTA DE MELHORIA NA ESTRUTURA DE REDES SEM FIO EM ESCOLAS PÚBLICAS NA MICRORREGIÃO DE ARARANGUÁ/ Ricardo Orige de Bem ; orientador, Juarez Bento da Silva, coorientador, Paulo Manoel Mafra, 2017.
81 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2017.

Inclui referências.

2. Tecnologias da Informação e Comunicação. 2. Redes sem fio. 3. Experimentação Remota. 4. Ensino Básico. 5. Tecnologias na Educação. I. Silva, Juarez Bento da. II. Mafra, Paulo Manoel. III. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. IV. Título.co

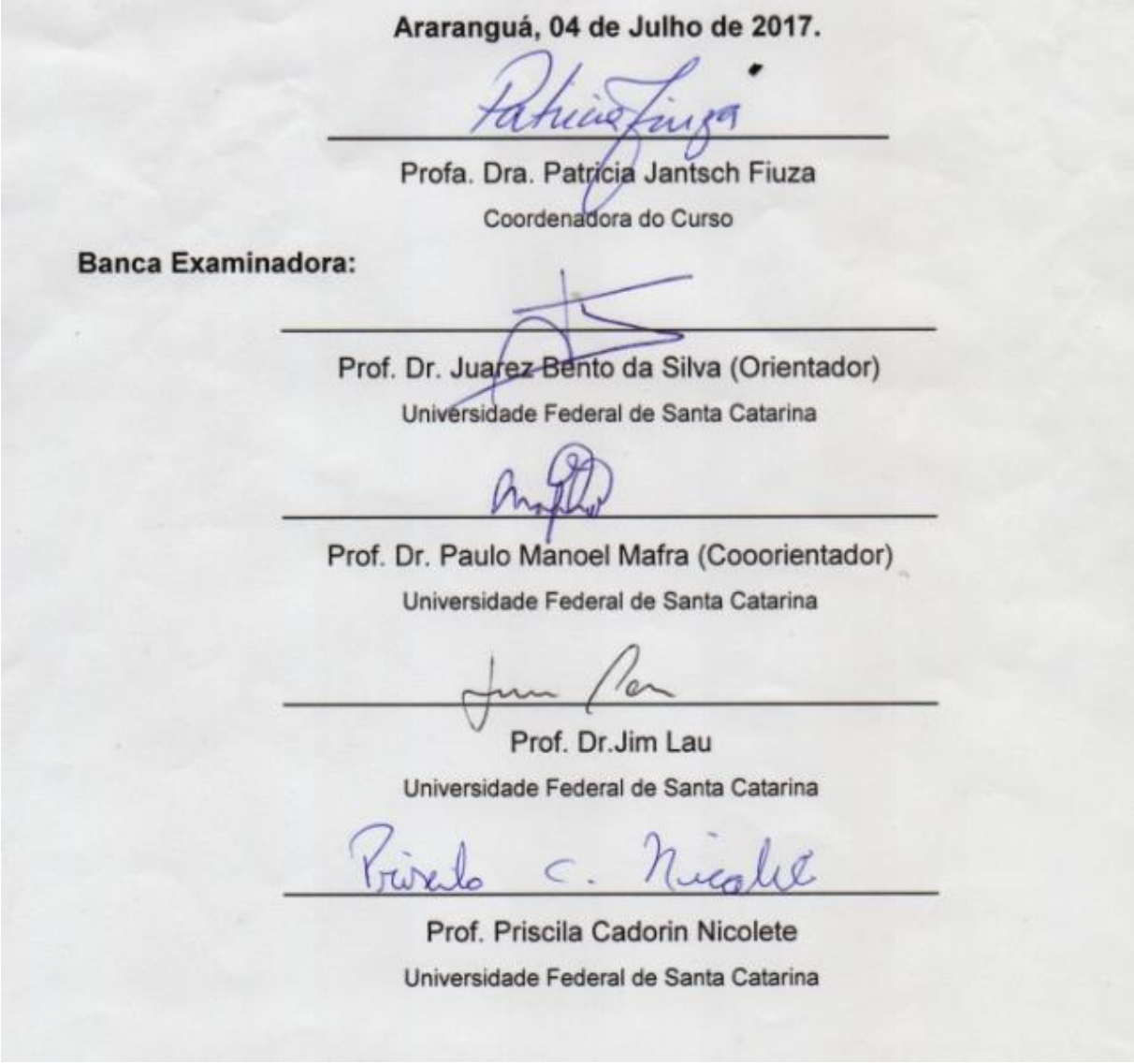
Lucas Vinícius de Oliveira

Ricardo Orige de Bem

Lucas Vinicius de Oliveira
Ricardo Orige de Bem

ANÁLISE E PROPOSTA DE MELHORIA NA ESTRUTURA DE REDES SEM FIO EM ESCOLAS PÚBLICAS NA MICRORREGIÃO DE ARARANGUÁ

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do grau de Bacharel em Tecnologias da Informação e Comunicação e aprovado em sua forma final pelo Campus Araranguá da Universidade Federal de Santa Catarina.



Araranguá, 04 de Julho de 2017.

Profa. Dra. Patricia Jantsch Fiuza
Coordenadora do Curso

Banca Examinadora:

Prof. Dr. Juarez Bento da Silva (Orientador)
Universidade Federal de Santa Catarina

Prof. Dr. Paulo Manoel Mafra (Cooorientador)
Universidade Federal de Santa Catarina

Prof. Dr.Jim Lau
Universidade Federal de Santa Catarina

Prof. Priscila Cadorin Nicolete
Universidade Federal de Santa Catarina

Dedicamos este trabalho a todos aqueles que nos apoiaram e nunca nos deixaram desistir

AGRADECIMENTOS

Eu começo agradecendo ao meu pai, Célio de Oliveira, que mesmo não estando mais comigo, sempre foi minha inspiração e o motivo de eu estar sempre buscando o melhor.

Agradeço também a minha mãe, Maristela Elias de Oliveira, por ser essa mulher exemplar, ótima mãe, nunca nos deixou faltar nada, sempre estando ao meu dispor para me auxiliar. Com certeza, parte de quem eu sou deve-se exclusivamente a ela.

Agradeço a Adriane Cristina Cantão Vieira, minha namorada, que sempre me incentivou a ir em frente, me motivando e me escutando nos momentos de dúvidas. Ela sempre esteve ao meu lado, entendendo o quão difícil pode ser terminar uma graduação.

Não posso deixar de agradecer também aos meus professores, que são aqueles que fazem uma universidade ser mais do que uma mera sala de aula.

(Lucas V. de Oliveira)

Gostaria de agradecer primeiramente a meu pai, por estar sempre presente em minha vida e não medir esforços para que eu pudesse levar meus estudos adiante, por sempre me apoiar e incentivar durante a graduação. Pai, sua presença foi fundamental para a conclusão dessa etapa importante de minha vida.

Agradeço minha mãe pelo amor incondicional e apoio durante a realização desse curso.

Agradeço meu irmão, por me auxiliar nessa empreitada, esclarecendo tópicos importantes no decorrer da faculdade.

Agradeço minha namorada, que conheci durante esta graduação e foi meu melhor presente de vida durante esses três anos de caminhada. Que está sempre me ajudando nas escolhas mais difíceis e me mostrando que eu posso sempre mais.

Agradeço a todos os colegas de faculdade, onde fiz amizades e sei que levarei para o resto da vida.

(Ricardo O. de Bem)

Agradecemos ao professor Paulo Manoel Mafra, pelo suporte e orientação durante esse trabalho de conclusão de curso, ficando sempre a disposição para nos auxiliar.

(Lucas V. de Oliveira e Ricardo O. de Bem).

“Um Homem dotado de lápis, papel e borracha, e sujeito a uma disciplina rígida, é na verdade uma máquina universal”.
Alan Turing

RESUMO

As redes sem fio alcançaram um patamar indispensável na comunicação humana. Diferentemente dos seus antecessores, as redes sem fio podem comportar diversos dispositivos em locais que anteriormente eram inviáveis de implementar em uma rede cabeada. Devido a sua praticidade as redes sem fio podem ser utilizados em diversas áreas como ambientes domésticos, corporativos e educacionais. O presente trabalho de conclusão de curso, teve como objetivo fazer um estudo da estrutura de redes sem fio em quatro escolas de educação básica da rede pública situadas na microrregião de Araranguá, Santa Catarina, a fim de identificar problemas e realizar a reestruturação da rede sem fio, prezando pela aplicabilidade e uso da experimentação para o ensino. A proposta deste trabalho está inserido no "*Promovendo a inclusão digital em escolas de Educação Básica da rede pública a partir da integração de tecnologias inovadoras de baixo custo no ensino de Ciências Naturais e Exatas"* que tem o foco na aprendizagem de ciências por alunos da rede pública e a capacitação dos docentes das escolas participantes no uso das tecnologias, para isso foram desenvolvido diversas práticas remotas. Entretanto, alguns problemas foram encontrados na estrutura atual dessas escolas impossibilidando o uso eficiente da tecnologia remota. Este trabalho teve o intuito de melhorar o acesso as redes sem fio, solucionando os problemas que impedem o desenvolvimento do projeto. Inicialmente foi feita uma análise prévia da situação em relação a infraestrutura em cada escola e então desenvolveu-se um estudo para a metodologia, para criar um embasamento teórico. Após a fase de metodologia, foi feita uma análise profunda da estrutura das escolas. Para isso, foram feitas diversas visitas aos locais, analisando toda a rede encontrada, focando principalmente em aspectos como sinal *wireless*, gerenciamento de senhas e localização dos *access points* (pontos de acesso). Seguido às visitas, foram desenvolvidas as plantas baixas de cada uma das quatro escolas, demonstrando as localizações dos dispositivos atuais. Com o conhecimento adquirido no levantamento em relação aos aspectos técnicos, foi proposto uma reestruturação de redes sem fio das escolas, atendendo a critérios de gerenciamento e segurança de rede e distribuição de sinal *wireless*.

Palavras-chave: Redes sem fio, Experimentação Remota, Ensino Básico, Tecnologias na Educação.

ABSTRACT

Wireless networks have reached an indispensable level in human communication. Unlike its predecessors, wireless networks can accommodate multiple devices in places that were previously unfeasible to implement over a wired network. Because of its practicality, wireless networks can be used in many areas such as home, corporate and educational environments. The objective of this undergraduate thesis is to study the structure of wireless networks in four public basic education schools located in the micro region of Araranguá, Santa Catarina, in order to identify problems and execute the restructuring the wireless networks of those schools, aiming on the applicability and use of experimentation for teaching. The objective of this thesis is inserted on "Promovendo a inclusão digital em escolas de Educação Básica da rede pública a partir da integração de tecnologias inovadoras de baixo custo no ensino de Ciências Naturais e Exatas" thesis, which has the focus on teaching science to public education students and the training of the teachers of the participating schools to use of those technologies, and for that reason we have created many remote activities. However, some problems were found in the current structure of those schools, making it impossible to use the remote technology efficiently. This undergraduate thesis has objective to improve the access to wireless technologies, solving the problems that prevented the accomplishment of the initial project. Initially, a preliminary analysis of the situation regarding infrastructure at each school was made and then a study was developed for the methodology in order to create a theoretical basis. After the methodology phase, a deep analysis of the structure of the schools was done. For this, several visits were made, analyzing all the network found, focusing mainly on aspects such as wireless signal, password management and location of access points devices. Following the visits, the floor plans of each of the four schools were developed, showing the locations of the current devices. With the knowledge acquired in the survey regarding technical aspects, it was proposed a restructuring of wireless networks of those schools, meeting the criteria of network management, security and wireless signal distribution.

Keywords : Wireless Networks, Remote Experimentation, Basic Education, Technologies in Education.

LISTA DE IMAGENS

LISTA TABELAS

LISTA DE SIGLAS

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AP	Access Point
ATM	Automatic Teller Machine
BSS	Basic Service Set
CHAP	Challenge Handshake Authentication Protocol
CIASC	Centro de Informática e Automação de Santa Catarina
DCF	Distributed Coordination Function
DS	Distribution System
EAP	Extensible Authentication Protocol
EEB	Escola de Educação Básica
ER	Experimentação Remota
ESS	Extended Service Set
ICP	Infraestrutura de Chaves Públicas
IEEE	Institute of Electrical and Electronics Engineers
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais
MAC	Media Access Control
MB	Megabyte
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol
NPS	Network Policy Server
OPKG	Open PacKaGe management
PAC	Protected Access Credentials
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In User Service
REXLAB	Laboratório de Experimentação Remota
RNP	Rede nacional de Pesquisa
TIC	Tecnologias da Informação e Comunicação
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
TKIP	Temporal Key Integrity Protocol
UFSC	Universidade Federal de Santa Catarina
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WLC	Wireless Lan Controller
WPA	Wi-Fi Protected Access
WRAP	Wireless Robust Authenticated Protocol

SUMÁRIO

1 INTRODUÇÃO

Este trabalho de conclusão de curso nasceu da necessidade e da oportunidade de levar as escolas de ensino público das cidades de Araranguá e Balneário Arroio do Silva o uso de laboratórios por meio da experimentação remota. Existe uma falta de equipamentos, estrutura e profissionais qualificados para atuar no ensino dos mais básicos conteúdos científicos. Como não existe uma forma rápida de modificar essa situação, buscou-se suprir as necessidades por meio da tecnologia remota. Vivemos em uma época na qual quase todos têm acesso a internet e podemos refletir então, que o caminho mais simples para contornar as necessidades básicas do ensino é utilizar de técnicas que façam uso da internet para transmitir esse conhecimento e dar acesso aos laboratórios que faltam dentro das escolas.

O Laboratório de Experimentação Remota (Rexlab) atua no município de Araranguá levando práticas remotas as escolas públicas, com o interesse de promover a tecnologia dentro da sala de aula. O Rexlab com o auxílio do programa InTecedu, vem mantêndo diversos projetos educacionais aplicados na microrregião de Araranguá. Esse programa, visa a integração da tecnologia dentro da educação básica da rede pública de ensino, dividindo-se em dois eixos principais: A capacitação de docentes no contexto das tecnologias e a integração das tecnologias dentro das atividades didáticas. O uso dessa tecnologia, se dá através de dispositivos móveis, que são utilizados para interação com ambientes virtuais de aprendizagem, objetos de aprendizagem, simuladores e experimentos remotos. O programa InTecedu proporcionou que diversos projetos fossem submetidos, entre eles, o projeto *Promovendo a inclusão digital em escolas de Educação Básica da rede pública a partir da integração de tecnologias inovadoras de baixo custo no ensino de Ciências Naturais e Exatas*, que disponibiliza materiais para melhoria das escolas, sendo a base para o tema deste trabalho.

Após a submissão e aprovação de uma proposta do RexLab de recursos para a melhoria na estrutura de rede das escolas da região de Araranguá e Balneário Arroio do Silva, ocorreu uma solicitação de diversos materiais para a melhoria da estrutura de rede dessas escolas.

Então, foi elaborado em colaboração com o professor Drº. Paulo Manoel Mafra a proposta de primeiramente realizar o levantamento da situação atual dos equipamentos utilizados nas seguintes escolas: Escola de Educação Básica Profa. Maria Garcia Pessi (Araranguá- - SC), Apolônio Ireno Cardoso (Balneário Arroio do Silva - SC), escola de Educação Básica de Araranguá (Araranguá) e Escola de Ensino Básico Profº. Otávio Manoel Anastácio (Araranguá). Obtendo assim os dados para que fosse ponderado um meio suprir as demandas com novos equipamentos e uma reestruturação da rede sem fio das escolas.

Com a verba do projeto usado de base pretende-se comprar onze *Access Points*, cabos de rede, servidor *raspberry* e quatro Roteadores de balanceamento de banda larga com capacidade agregar diversos links de acesso a internet e fazer sua distribuição. Além dos *Access Point* e roteadores disponíveis, o projeto conta com a proposta de novo link contratado de acesso de 15 *megabyte* por segundo (MB/s). Então, com a disposição de novos equipamentos e um novo serviço, foi elaborada uma proposta para solucionar os problemas nas redes das escolas selecionadas.

1.1 DEFINIÇÃO DO PROBLEMA

Ainda que os processos de ensino por meio de experimentação remota estejam consolidados, dentro das escolas faltam recursos que possam prover o acesso dos jovens às atividades que envolvem esta tecnologia, ou seja, tem-se um problema estrutural. Problema esse que não se resume somente a qualidade de sinal wireless e velocidade de conexão, mas também nas condições dos equipamentos, as quais foram encontrados os seguintes casos:

- Qualidade dos Access Points - Alguns equipamentos são de baixa qualidade, afetando diretamente no raio de alcance de sinal wireless;
- Equipamentos mal distribuídos - A localização de alguns equipamentos não considera a estrutura atual da escola, tornando ineficaz a distribuição de sinal wireless para todas as salas;
- Falta de equipamentos – Existe uma falta de equipamento para cobrir a área necessária para as práticas pedagógicas

- Falta de manutenção – Algumas escolas possuem *Access Points* instalados que não distribuem sinal, estão somente conectados na rede elétrica;
- O uso de Repetidores de sinal – Algumas escolas utilizam repetidores de sinal, afetando diretamente na sua qualidade;
- Gerenciamento de senhas de rede - Nenhuma escola possui um gerenciamento eficaz de rede, acarretando em vazamentos de senhas e sobrecarregando a rede.

A partir da definição dos problemas de rede encontrados nas escolas, surgem algumas perguntas. Como melhorar a infraestrutura de rede atual das escolas municipais e estaduais na microrregião de Araranguá? O processo de reestruturação de redes sem fio é viável?

1.2 OBJETIVO GERAL

O Objetivo geral deste trabalho de conclusão de curso é analisar e fazer uma proposta de reestruturação nas redes sem fio das seguintes escolas de ensino básico: Escola de Educação Básica Profº. Apolônio Ireno Cardoso - pertencente ao município de Balneário Arroio do Silva, Escola de Educação Básica Profª Maria Garcia Pessi, Escola de Educação Básica de Araranguá e a Escola de Educação Básica Profº Otávio Manoel Anastácio pertencente a Araranguá, adaptando às mudanças baseadas nas necessidades de cada uma.

1.2.1 OBJETIVOS ESPECÍFICOS

De modo a atingir o objetivo principal, foram definidos os seguintes objetivos específicos:

- Coletar dados a respeito da estrutura das escolas pesquisadas;
- Analisar a estrutura das redes wireless das escolas;
- Melhorar a estrutura de distribuição de wireless, baseado em cada caso;

- Definir o gerenciamento de senhas das escolas, levando em consideração os métodos apropriados de proteção e autenticação;
- Documentar a situação encontrada e as mudanças a serem aplicadas.

1.3 JUSTIFICATIVA E MOTIVAÇÃO

Com o avanço e inclusão das tecnologias, os métodos de educação também se modificaram e evoluíram, tornando-se aliados importantes para melhorar o aprendizado, atualizando os métodos de ensino. “As mudanças sociais e culturais estão abrindo caminhos para novas formas de aprender e ensinar para além do quadro e giz.” (HECK et al., 2016). Atualmente a grande maioria das pessoas estão conectadas de alguma forma a internet, celulares, tablets e computadores fazem parte do cotidiano Brasileiro. Consequentemente é natural então que se tentem iniciativas para incluir as tecnologias dentro da sala de aula.

O Laboratório de Experimentação Remota mantém alguns projetos visando a utilização de experimentos remotos por meio do uso de tablets e dispositivos móveis nas escolas de Araranguá e Balneário Arroio do Silva. Entretanto, apesar da aceitação das instituições de ensino, não existem condições favoráveis para um uso pleno da tecnologia remota. Mesmo existindo sinal wireless nos locais, não há como suportar cerca de 30 tablets conectados na rede disponível.

Por já existirem iniciativas com pessoas engajadas no uso tecnológico nas escolas, é crucial que se pense em uma reestruturação dos locais visando acabar com as barreiras que impedem alunos e professores de empregar a tecnologia dentro da sala de aula.

1.4 METODOLOGIA

Este subcapítulo tem o objetivo de descrever os procedimentos metodológicos utilizados ao longo deste trabalho de conclusão de curso.

1.4.1 ESPECIFICAÇÃO DA PESQUISA

Inicialmente podemos classificar a pesquisa, quanto ao seu nível de profundidade como uma pesquisa exploratória, que busca o desenvolvimento de uma ideia, a partir de problemas encontrados. Então, se faz “ (...) desencadear um processo de investigação que identifique a natureza do fenômeno e aponte as características essenciais das variáveis que se quer estudar” (KOCHE, 1997, p. 126).

A pesquisa utilizada neste trabalho baseia-se em coletar dados acerca da realidade pesquisada e analisar os dados encontrados interpretando-os com base na fundamentação teórica com o objetivo de encontra r soluções para os problemas encontrados, ou seja, é também uma pesquisa de campo.

> A pesquisa de campo é o tipo de pesquisa que pretende buscar a informação diretamente com a população pesquisada. Ela exige do pesquisador um encontro mais direto. Nesse caso, o pesquisador precisa ir ao espaço onde o fenômeno ocorre, ou ocorreu e reunir um conjunto de informações a serem documentadas [...]. (GONSALVES, 2001, pg. 67)

O tema da pesquisa pode ser abordado de maneira qualitativo, pois foca-se principalmente no estudo das particularidades de cada local pesquisado. Na pesquisa qualitativa, a análise dos resultados é feita de forma intuitiva e indutiva pelo pesquisador, não requerendo uso de métodos estatísticos como é feito na pesquisa quantitativa. Existe uma maior preocupação na interpretação dos fenômenos e nos resultados. (GODOY, 1995).

A aplicação do conhecimento é feita na forma de uma pesquisa aplicada, que objetiva, a partir do conhecimento adquirido, desenvolver técnicas para resolver problemas específicos. Portanto, ao obter uma base sólida na fundamentação, pode-se utilizá-la na elaboração de soluções para os problemas encontrados nas escolas pesquisadas. (FREIRE, 2013)

Os procedimentos técnicos que foram utilizados são pesquisa bibliográfica e estudo de caso.

Uma pesquisa bibliográfica, possui a capacidade de prover ao pesquisador uma forma de se informar e assim poder analisar diversos pontos de vista sobre o determinado assunto, podendo se desprender de uma bolha social.

De forma sucinta, afirma-se que com uma pesquisa bibliográfica pode-se:

> (...) obter informações sobre a situação atual do tema ou problema pesquisado; conhecer publicações existentes sobre o tema e os aspectos que já foram abordados; verificar as opiniões similares e diferentes a respeito do tema ou de aspectos relacionados ao tema ou ao problema de pesquisa (SILVIA, MENEZES. 2001)

A principal motivação para pesquisa bibliográfica é a capacidade de analisar livros e artigos científicos a fim de encontrar informações sólidas, acerca do tema.

O estudo de caso, segundo Heerdt e Leonel (2007), é definido como “estudo exaustivo, profundo e extenso de uma ou de poucas unidades, empiricamente verificáveis, de maneira que permita seu conhecimento amplo e detalhado. ”

1.4.2 ETAPAS DA PESQUISA

Inicialmente foi feito um levantamento das metodologias de pesquisa apropriadas para o trabalho de conclusão, resultando na pesquisa bibliográfica.

Com o uso da pesquisa bibliográfica pode-se aplicar um levantamento de referenciais teóricos indispensáveis para o tema. Para fundamentar o conhecimento em redes, foi estudado Kurose e Ross (2010) e Tanenbaum (2003), com os livros "Redes de Computadores e a Internet: Uma Abordagem Top - Down", e "Redes de Computadores." Já para experimentação remota, foi seguido principalmente as publicações do laboratório de experimentação remota (REXLab), encontradas no próprio site do laboratório, que constam com diversos artigos do Profº Dr. Juarez Bento da Silva.

Após a pesquisa bibliográfica, foi estudada qual ferramenta melhor se adaptaria a uma situação de análise de cada escola individualmente, de todas as pesquisadas, o estudo de caso foi a que melhor se adaptou.

Para o estudo de caso, foi feito um levantamento da estrutura encontrada e uma análise de seus equipamentos e documentação dos mesmos. Demostrando cada problema encontrado individualmente, bem como as particularidades dos locais.

Após a análise da estrutura, com o uso do *software* CorelDRAW, foram criadas plantas para cada escola, com todas as salas e um mapeamento do sinal das redes sem fio. A medição de sinal *wireless* foi feita com o uso de smartphones, que mediante

a funcionalidade de conexão, puderam demostrar o sinal disponivel em cada sala das escolas analisadas.

Logo, com a finalização das plantas, partiu-se para um plano de desenvolvimento das propostas, pois com a base teórica e a análise dos locais, os dados podem ser analisados e assim encontrar soluções para os problemas descritos neste trabalho.

1.5 ORGANIZAÇÃO DO TEXTO

O elemento textual do trabalho está dividido em cinco partes, introdução, revisão de literatura, desenvolvimento, proposta e resultados.

A introdução apresenta o assunto e a proposta do trabalho, bem como nossos objetivos, prezando pelo entendimento do leitor. Apontamos a ideia geral proposta e como foi feita sua aplicação, também é mostrado como foi fundamentado cientificamente a pesquisa.

O **Capítulo 2** apresenta revisão de literatura, buscando fundamentar as ideias, ampliando a visão teórica acerca da proposta, dando o embasamento para a discussão do tema. Nela é demostrado o que são as redes sem fio, discorrendo um pouco sobre seu histórico até chegarmos à atualidade. Neste capítulo é discutido os diversos mecanismos de proteção e de autenticação das redes 802.11, apontando suas características e principais vantagens, bem como um levantamento de sistemas embarcados para Access Points. Por último, é explicada sobre a experimentação remota, sua proposta, ideais e históricos, remontando seu início e projetos de sucesso.

O **Capítulo 3** apresenta elementos iniciais da pesquisa aplicada, bem como explicações sobre o rumo tomado. Esse capítulo apresenta a infraestrutura de redes das quatro escolas de Araranguá e Balneário Arroio do Silva. Foi feito um levantamento da estrutura encontrada e uma análise de seus equipamentos, onde foi elaborada uma planta para cada escola exibindo a localização dos dispositivos, medindo seus respectivos sinais de wireless, além do gerenciamento de senhas atual.

O **Capítulo 4**, apresenta as propostas de melhoria para cada escola, examinando suas necessidades, como novos dispositivos implementados, nova proposta de gerenciamento de senhas e segurança.

O **Capítulo 5** finaliza o trabalho, com as considerações finais e conclusão do trabalho.

2 REVISÃO DA LITERATURA

Este capítulo tem como objetivo descrever os principais conceitos relacionados a redes sem fio, bem como seus mecanismos de proteção, autenticação, sistemas embarcados abertos para *access points*, experimentação remota e sua aplicação nas escolas públicas.

2.1 REDES SEM FIO

As redes sem fio surgiram da necessidade e desejo de existir comunicação em qualquer hora ou lugar com acesso rápido e compartilhado. Diferente dos modelos físicos, às redes sem fio não necessitavam de todo um aparato e terminais com cabeamento para o uso de um dispositivo, além de evitar uma total reestruturação para sua implementação.

Com um início tímido na década de 2000, as redes sem fio foram preenchendo diversas lacunas encontradas pelo seu antecessor. Apesar dos empecilhos atuais, existem grandes investimentos em estudos científicos em soluções que demandam por exemplo uso em tempo real das redes. (CORRÊA, 2006). Segundo Tanenbaum (2003, p. 24), os dispositivos móveis constituem um dos segmentos de mais rápido crescimento da indústria de informática e pela sua comodidade todos querem se manter conectados mesmo longe de casa ou em trânsito.

Além de facilitar a conexão de uso próprio, as redes sem fio tem utilidade nas mais diversas áreas, como nas universidades, onde são feitas instalações de redes sem fios no campus, possibilitando que os alunos tenham acesso e executem tarefas como, consultar a biblioteca e responder e-mails em qualquer lugar. Outra função importante é seu uso nos exércitos, no qual talvez não seja possível contar com uma infraestrutura apropriada para uso de uma rede local, tornando a melhor opção carregar o seu próprio equipamento. (TANENBAUM, 2003).

As redes sem fio mantém uma relação de proximidade com a computação móvel, porém, distanciam-se no que se refere a sua utilização. “Computação móvel é a capacidade de o usuário continuar conectado enquanto se movimenta, já as redes

sem fio têm como objetivo a utilização de outro meio que não seja por cabo.” (JASPER, 2010).

Com a propagação da tecnologia wireless, diversas novas possibilidades surgem, como Tanenbaum (2004, pg.25) cita sobre os Parquímetros: “Esses equipamentos poderiam aceitar cartões de crédito ou débito, com verificação instantânea, pelo link sem fio.”. Tal tecnologia poderia ser aplicada para confirmar a presença de um automóvel e relatar o término do prazo, tudo sem precisar de equipamentos fixos, mantendo uma melhor fiscalização do estacionamento e monitoramento das vagas.

Além de supostos usos futuros, podemos encontrar diversos tipos de redes sem fio em nosso cotidiano, entre elas as mais comuns são as redes wi-fi. Seja nos shoppings, lojas, mercados ou até mesmo em meios de transportes como aviões, as redes *wi-fi* caíram no gosto popular e hoje são necessárias em qualquer tipo de empreendimento ou lazer.

Existe muita confusão com os termos *wi-fi* e *wireless*, diversas pessoas confundem um com o outro ou pensam que tais termos são sinônimos. A conexão *wi-fi* provém do padrão 802.11 estabelecido pela IEEE (*Institute of Electrical and Electronics Engineers*) homologado no final da década de noventa. Tal conexão é feita a partir de ponto onde exista previamente uma conexão cabeada juntamente com um transmissor que fará o serviço de distribuição do sinal de internet pelo ar. (ENGST & FLEISHMAN, 2005)

> Em 1999 o IEEE finalizou o padrão 802.11b (11Mbps a 2,4GHz). Em 2002, foi distribuído ao mercado o 802.11a (54Mbps a 5GHz), que é incompatível com o padrão 802.11b. No mesmo ano, foi ratificado o padrão 802.11g (54Mbps a 2,4GHz), que opera na mesma velocidade do 802.11a e na mesma frequência do 802.11b. (ENGST & FLEISHMAN, 2005)

O Wireless com seu significado literal “sem fio” caracteriza qualquer tipo de conexão para transmissão de sinal que não utilize cabos ou fios, ou seja, *wi-fi*, *bluetooth* e infravermelho se enquadram nesse tipo de tecnologia. Inclusive como um exemplo lúdico, suponhamos que durante diálogo entre duas pessoas, uma espécie

de conexão sem fio é mantida, pois, a onda sonora criada pela corda vocal não utiliza de nenhum cabo até chegar ao ouvido do receptor. (ARTHAS, 2010).

Evoluindo de diversas maneiras, as redes *wireless* conseguiram com o tempo se consolidar em diversos nichos, e em poucos anos se difundir de diversas maneiras. Tal evolução proporcionou grandes transformações no seu uso, dentre os diversos tipos, a mais comum é a rede local sem fio, ou WLAN (*Wireless Local Area Network*), utilizada pela maioria da população.

> Redes Locais sem Fio ou WLAN (Wireless Local Area Network), Redes Metropolitanas sem Fio ou WMAN (Wireless Metropolitan Area Network), Redes de Longa Distância sem Fio ou WWAN (Wireless Wide Area Network), redes WLL (Wireless Local Loop) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (Wireless Personal Area Network). (ARTHAS, 2010)

Segundo Arthas (2010), “as aplicações de rede estão divididas em dois tipos: aplicações indoor e aplicações outdoor.”

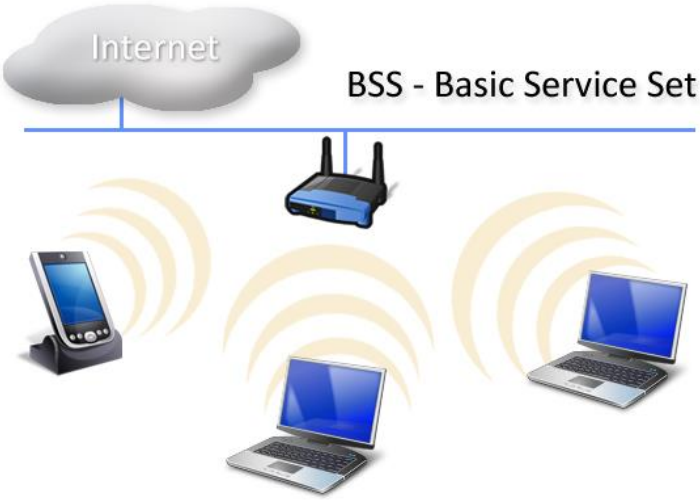
Uma aplicação *indoor* é utilizada geralmente para pequenas áreas como residências e escritórios e é uma rede focada a um número reduzido de usuários. Uma das vantagens desta aplicação, é que por cobrir um espaço menor que a *outdoor*, a possibilidade de perda de sinal também se torna reduzida, pois existe uma incidência menor de frequências próximas. Grande parte das redes *indoor* fazem uso de padrões mais simples como o 802.11b e 802.11g e por ser uma rede menos complexa, usuários com pouco conhecimento conseguem fazer uma instalação de redes sem fio com êxito. (CAMARGO & CORSINI, 2010)

Já a *outdoor* por sua vez, é utilizada em áreas maiores com diversos pontos interligados, como uma empresa fazendo ponto a ponto até a matriz. Devido à área de alcance ser imensamente maior quando comparada com a *indoor*, sujeita a poucos metros, as aplicações *outdoor* geralmente medem quilômetros de um ponto a outro. Nestas distâncias a chance de interferência se torna maior e graves problemas podem ocorrer quando um sinal entra no raio de outro.

Meneses *apud* Arthas (2009) define que a topologia de uma rede 802.11 pode ser composta pelos seguintes elementos:

- **AP** - *Access-point* - É um dispositivo conectado à rede convencional que coordena a comunicação entre os clientes, tem a função de disponibilizar o acesso a rede de forma sem fio pela distribuição de sinal.
- **BSS** - *Basic Service Set* - É uma rede que consiste de um *Access-point* que se comunica um ou mais clientes à internet, Figura 1.

Figura 1: Ilustração de um BSS



Fonte: Site WLAN - Topologias 802.11[1]

- **STA** - *Wireless Lan Stations* - É considerado o dispositivo que está conectado a rede.
- **ESS** - *Extended Service Set* - São os conjuntos de células BSS (*Basic Service Set)* os quais se interceptam e cujo APs estão conectados na rede convencional. Nestas condições uma STA pode se movimentar de um BSS para outro sem se desconectar da rede, fazendo o processo conhecido por *Roaming*.

O funcionamento de uma rede sem fio é construído a partir de um AP com conexão para uma rede tradicional, de ethernet local. Os AP conservam uma função

[1] Disponível em https://www.wlan.com.br/?p=453

parecida com o hub da rede com fio, retransmitindo os pacotes de dados, atingindo todos os dispositivos da rede. (ARTHAS, 2010)

2.1.1 MECANISMOS DE PROTEÇÃO EM REDES SEM FIO

A facilidade no uso de redes sem fio traz ao usuário, inúmeros benefícios, entretanto, as questões sobre segurança ficam evidentes. Segundo Ohtman (2003), nas redes sem fio, o sinal se propaga no ar, se espalhando a centenas de metros de distância utilizando apenas um dispositivo móvel, tornando a rede sem fio inerentemente vulnerável a interceptação.

Existem basicamente dois tipos de reações por parte do usuário da rede em relação às redes sem fio. A não aceitação da tecnologia por medo ou desconhecimento das implicações resultantes sobre a inexperiência no uso de mecanismos de segurança de rede e a demasiada aceitação e impulsividade no seu uso, sem compreender a tecnologia, seus riscos e medidas de segurança recomendadas (RUFINO, 2007).

Como forma de melhorar a segurança no uso de redes sem fio, existem vários mecanismos de proteção, denominados protocolos de segurança.

2.1.1.1 ENDEREÇO MAC

Ao criar uma rede doméstica, o administrador pode optar a várias possíveis opções para a configuração, no entanto, as opções mais comuns são: Configurar o *Access Point* deixando o sinal em aberto, dando a possibilidade ao acesso à rede para qualquer usuário; configurar o *Access Point* com senha, passando essa senha apenas para pessoas em que pretende dividir a rede e limitar o acesso à rede através do endereço MAC (*Media Access Control address*). (GUISS, 2010).

Endereço Mac é um endereço físico de números em formato hexadecimal composto de 48 bits e se encontra gravado em um dispositivo de rede (MENEGOTTO, 2011).

Teoricamente, cada dispositivo de rede deveria ter um endereçamento MAC único, porém, alguns dispositivos de redes eram fabricados com o mesmo número e

os fabricantes concediam um *software* que cadastram um MAC único de uma lista que acompanhava um pacote de placas (RUFINO, 2007).

Configurar uma rede sem fio com esse mecanismo de segurança, possui como principal vantagem o estabelecimento de rede apenas para usuários, cujo endereço MAC de seu equipamento está cadastrado. Além de selecionar os usuários no uso da rede sem fio, torna muito mais trabalhoso para um intruso invadir e utilizar a rede sem autorização.

Por outro lado, existe uma desvantagem que segundo Rufino (2005) apud Gimenes (2005) é que o método faz a autenticação somente do equipamento, esquecendo assim o usuário, ou seja, torna possível que alguém não autorizado faça uso da rede com um equipamento autorizado por ela anteriormente.

Outra desvantagem está no limite da quantidade de endereços MAC cadastrados no dispositivo, tornando ineficiente em lugares em que é necessário cadastrar muitos equipamentos, sem contar a necessidade de cadastrar manualmente um a um.

2.1.1.2 WEP

Diferente das redes cabeadas, as redes sem fio estão sujeitas a uma série de problemas em relação à segurança por ter uma maior vulnerabilidade. Pensando nessa característica, o padrão 802.11 estabeleceu um conjunto adicional de procedimentos de segurança denominado WEP (*Wired Equivalent Privacy*) (SIFURO, 2005).

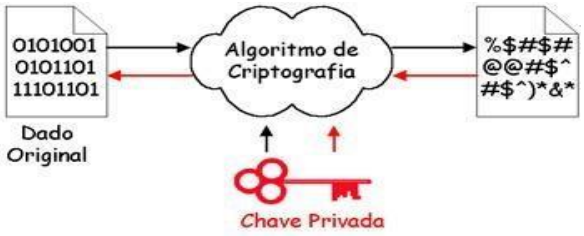
O protocolo WEP utiliza algoritmos concordantes, os quais o emissor e o receptor fazem uso da mesma chave criptográfica para encriptação de texto puro e decriptação de texto cifrado nas mensagens trafegadas na rede (RUFINO, 2007).

> A segurança WEP é composta de dois elementos básicos : Uma chave estática, que deve ser a mesma em todos os equipamentos de rede, e um componente dinâmico, que, juntos, irão formar a chave usada para cifrar o código. O protocolo não define de que forma essa chave deve ser distribuída, portanto a solução convencional é também a mais trabalhosa, em que a chave é cadastrada manualmente em todos os equipamentos (RUFINO,2007)

Esse tipo de mecanismo foi estabelecido nas redes sem fio no intuito de equiparar sua segurança às redes *ethernets*. Mas, existem diversos programas que tem a capacidade de desencriptação de chave ao monitorar o tráfego da rede no decorrer de algumas horas (RUFINO, 2005 apud GIMENES, 2005).

Esse protocolo foi um dos primeiros a ser lançado nas redes sem fio e amplamente utilizado. Ainda que tal protocolo possua fraquezas no seu uso, já garante um nível básico de proteção.

Figura 2: Algoritmo de criptografia simétrico



Fonte : Site Assinatura Digital, Tipos de Criptografia [2]

2.1.1.3 WPA

Ao evidenciar os problemas do protocolo WEP, Dermatini (2013) afirma que o protocolo WPA (*Wi-Fi Protected Access*) foi adotado formalmente no ano de 2003, trazendo encriptação de 256 bits entrando como protocolo padrão da indústria. Nessa atualização foi incrementado pacotes para verificar alterações e possíveis invasões, além de ferramentas adicionais que ajudaram a melhorar a segurança. (WPA, 2017)

> Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves. (WPA, 2017)

Para ativar o WPA, cada usuário deve entrar com uma única senha. Após a ativação, a senha irá mudar frequentemente para prevenir acessos não autorizados à rede. Esta é a diferença da WPA para WEP, já que a WEP utiliza uma única chave estática de criptografia (DUARTE, 2010).

[2] Disponível em :https://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html#Topic6

Ainda que tenha ocorrido um grande esforço para solucionar os problemas do protocolo WEP, algumas falhas na sua implementação o tornam vulnerável. (DUARTE, 2010)

> O MIC possui um mecanismo de proteção para evitar ataques de força bruta, porém esse mecanismo acarreta um ataque de negação de serviço (DoS). Quando dois erros de MIC são detectados em menos de um minuto o AP cancela a conexão por 60 segundos e altera a chave de integridade. Portanto, com uma simples injeção de pacotes mal formados é possível fazer um ataque de negação de serviço. (DUARTE, 2010)

.Em vista dos problemas vistos no decorrer de sua usabilidade, foi criado um protocolo responsável por cobrir as falhas e vulnerabilidades do WEP e do WPA, conhecido como WPA2.

2.1.1.4 WPA2

Como um sucessor, o WPA2 ratificado em 2004, faz uso das qualidades do WPA juntamente com novos mecanismos que melhoraram significativamente a segurança dos dados.

Segundo Larrosa et al. (2013), o padrão utiliza o protocolo AES (*Advanced Encryption Standard*), que tem a função de fazer um algoritmo de criptografia mais forte tomar o lugar ao algoritmo do protocolo WEP.

> Como o TKIP do WPA, o AES permite a descoberta de uma chave de criptografia de difusão ponto a ponto inicial exclusiva para cada autenticação, bem como a alteração sincronizada da chave de criptografia de difusão ponto a ponto para cada quadro. Como as chaves AES são descobertas automaticamente, não há necessidade de se configurar uma chave de criptografia para o WPA2. O WPA2 é a modalidade de segurança sem fio mais forte (GIMENES, 2005)

Embora a WPA2 seja o protocolo que oferece a maior segurança atualmente, tal protocolo também tem desvantagens. O algoritmo de criptografia AES exige um maior processamento de dados para sua execução, então seu uso é indicado para usuários que necessitam de um alto padrão de segurança de redes como, por exemplo, organismos governamentais. No entanto, esta desvantagem não se torna tão relevante, já que as máquinas atuais são capazes de sustentá-lo tranquilamente.

2.1.2 MECANISMOS DE AUTENTICAÇÃO EM REDES SEM FIO

Autenticação é o mecanismo responsável pela confirmação da procedência de uma mensagem através da verificação da identidade em que um processo confirma que seu parceiro na comunicação é quem deve ser, e não um impostor (TANENBAUM, 2003). Fazendo uma analogia, como seres humanos, fizemos autenticação de uns aos outros através de várias maneiras: Reconhecemos pessoas pela voz, pelo rosto, somos autenticados por um oficial da alfândega, onde é comparado nossos dados com a do passaporte, entre vários outros exemplos. (KUROSE & ROSS, 2010).

Segundo Rufino (2007) a maneira tradicional de adicionar segurança a um usuário em uma rede sem fio, é promover sua autenticação junto do equipamento que utilizará na rede, sendo esse equipamento muitas vezes baseado em autenticação por senhas fixas, porém existindo várias alternativas desde senhas dinâmicas até certificação digital.

Para Tanenbaum (2003) confirmar a identidade de um processo remoto, com a presença de um intruso, é de extrema dificuldade e exige protocolos complexos de criptografia.

Como existem algumas ambiguidades, é comum confundir autenticação com autorização. Para Tanenbaum (2003), a autenticação trata com a questão de determinar se um usuário está ou não se comunicando com algum processo específico e autorização tem como objetivo, se preocupar com o que esse processo pode ou não fazer.

A seguir serão abordados alguns dos vários mecanismos de autenticação existentes usados nas redes de computadores.

2.1.2.1 IEEE 802.1X

O padrão IEEE 802.1x foi desenvolvido para contornar aspectos falhos de segurança, como segmentos da rede que não podem ser verificados. Para tal, ele provê um processo de autenticação entre os clientes da rede e o ativo que se encontram conectados com conexões sem fio, seja por um *switch* ou por um *AP*.

Para isso, o IEEE 802.1x utiliza um modelo central de arquitetura de controle integrada ao padrão de AAA (*Authentication, Authorization and Accounting*) que são componentes fundamentais para o controle completo da rede. Em suma, o IEEE 802.1X “define porta como sendo um ponto de conexão à LAN, podendo ser uma porta física em redes cabeadas, ou uma porta lógica, como no caso da associação entre um dispositivo sem fio e o ponto de acesso.“ (BARROS & FOLTRAN. 2008).

Existem diversos métodos de autenticação encontrados nas redes 802.11 e devido a grande diversidade destes, acabam por gerar também diversos problemas de autenticação. Neste contexto, o padrão IEEE 802.1x se destaca, garantindo uma compatibilidade entre os protocolos TKIP (*Temporal Key Integrity Protocol*) e o padrão de criptografia AES.

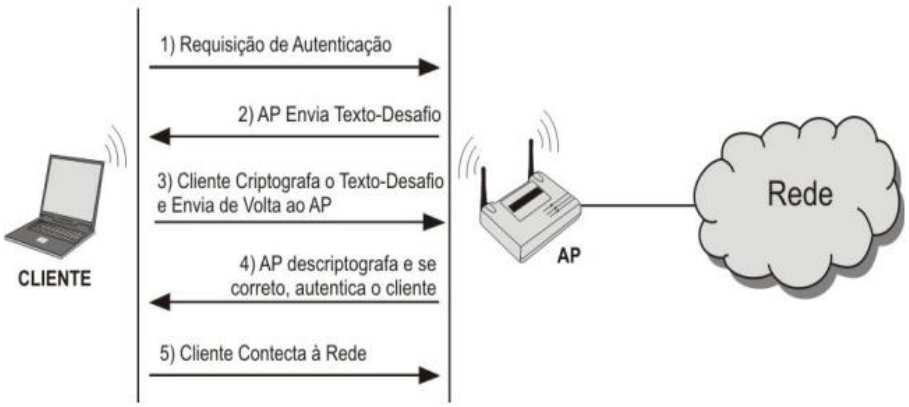
Segundo Barros e Foltran (2008, p.4), “utilizando o EAP é possível ter independência de mecanismos de autenticação PPP, sendo assim uma alternativa interessante para interligação de redes vista a sua capacidade de adaptação a novos mecanismos.”.

2.1.2.2 AUTENTICAÇÃO BASEADA EM CHAVE COMPARTILHADA

O protocolo de chave compartilhada é baseado em um princípio encontrado em muitos protocolos de autenticação: o emissor envia um número aleatório ao receptor, que em seguida o transforma de algum modo especial e retorna o resultado (TANENBAUM, 2003). Em outras palavras, a autenticação de chave compartilhada requisita uma chave compartilhada em que será distribuída às estações antes de tentar a autenticação (GAST, 2005).

Segundo Gast (2005), o fundamento teórico crucial da autenticação de chave compartilhada é que para confirmar a procedência de uma mensagem enviada pelo cliente, um desafio é lançado e uma resposta prova a posse da chave compartilhada. O processo de autenticação de uma chave compartilhada pode ser representado pela Figura 3.

Figura 3: Comunicação WEP utilizando chave compartilhada



Fonte: Monografia *A Evolução dos Protocolos de Segurança das Redes Sem Fio: do Wep ao Wpa2 Passando Pelo Wpa* (DUARTE, 2010)[3]

Segundo Duarte (2010):

1. O Emissor envia uma mensagem solicitando autenticação por *shared key* ao Receptor (*Acces Point*);
2. O Receptor responde a mensagem contendo um desafio;
3. O Emissor cifra o desafio com sua chave WEP e retorna uma mensagem com o resultado;
4. Se o Receptor decifrar a chave e obtiver o desafio original, ele responde ao Emissor autorizando acesso.

2.1.2.3 RADIUS

A automação de recursos possibilitou ao usuário, utilizar serviços através de aplicativos em que antes era possível resolver apenas presencialmente. Os usuários possuem contas em diversas redes sociais, e-mail, entre outros serviços em que o usuário utiliza a autenticação como método de validação de seus dados pessoais. Para Chaves (2010) a forma de autenticação para esses recursos é através do *login*

[3] Disponível em: https://www.esab.edu.br/wp-content/uploads/monografias/carlos-anderson-andrade-duarte.pdf

e senha em que ao inserir os dados corretamente, o computador faz a autenticação dos dados através da verificação de autenticidade do usuário, verifica as devidas permissões e retorna o resultado. Todo esse processo é função do protocolo de autenticação Radius.

> Este protocolo usa um cenário de cliente-servidor em que o cliente, designado de NAS (Network Access Server) envia pedidos de autenticação dos utilizadores e o servidor responde. As respostas do servidor poderão ser em forma de desafios, de aceitação ou rejeição do utilizador. O RADIUS é muito utilizado por fornecedores de acesso à Internet, bem como por organizações que pretendam um sistema de autenticação centralizado para autenticar o acesso à rede e aos seus recursos. O RADIUS apresenta ainda a vantagem de poder juntar informação referente à troca de dados e sessões de cada utilizador, a que se chama de contabilização. (ANTUNES, 2009)

Segundo Barros e Foltran Junior (2008), o servidor verifica as informações recebidas do cliente RADIUS, e em seguida faz sua autorização e autenticação dos dados, mandando uma mensagem ao cliente com o resultado do acesso (negado ou autorizado) e posteriormente faz a liberação de acesso à rede pelo requisitado conforme a figura 4.

Figura 4: Processo de autenticação e autorização RADIUS

Fonte: Artigo Autenticação IEEE 802.1x em Redes de Computadores Utilizando TLS e EAP (BARROS & FOLTRAN JUNIOR, 2008)[4]

2.1.2.4 EAP

A WPA e a WEP apresentam duas versões distintas. A maior diferença entre esses dois mecanismos de proteção é que enquanto a WEP (*Wired Equivalent*

[4] Disponível em: http://www.4eetcg.uepg.br/oral/62_1.pdf

Privacy) funciona a partir da distribuição da chave secreta entre o emissor e receptor a WPA (*Wi-Fi Protected Access*) requer um método de autenticação à parte, este é realizado pelo EAP (PAIM, 2011).

> O 802.1x depende de um Servidor RADIUS, de uma autenticação de rede e de um serviço de autorização para verificar as credenciais do cliente na rede. O 802.1x utiliza o EAP como meio de fazer o pacote de conversação da autenticação entre diversos componentes da solução, e gerar as chaves usadas para proteger o tráfego entre os clientes e o hardware de acesso da rede (SIFURO, 2005).

O EAP (*Extensible Authentication Protocol*) é utilizado para fazer a seleção de um determinado mecanismo de autenticação levando em consideração as informações que o autenticador solicitar para determinar o método apropriado de autenticação a ser utilizado. Em vez de exigir a atualização do autenticador para suportar cada novo método de autenticação, o EAP autoriza a utilização de um servidor de autenticação do *backend* que pode fazer a implementação dos métodos de autenticação. (ABOBA et al., 2004)

Segundo Oliveira (2007), “O framework 802.1x/EAP, na utilização em redes sem fio, estabelece um ambiente flexível e seguro levando em consideração aos esquemas de autenticação usados na atualidade.”

2.1.2.5 EAP - TLS

Segundo Gast (2005), o protocolo EAP-TLS (*Extensible Authentication Protoc l- Transport Layer Security*) foi projetado para uso em links que estão sujeitos a espionagem. Tal protocolo possui um procedimento de autenticação em que é apresentado um canal de criptografia entre um cliente (TLS), sendo este um padrão amplamente utilizado nas redes sem fio e um dos mais seguros disponíveis EAP, além de possuir grande suporte, agregando a todos os fabricantes de hardware, software e LAN sem fio. (MORAIS, 2016)

Oliveira (2007, p. 50) informa que “A sua implementação requer o suporte EAP-TLS no servidor RADIUS, e ainda, por ser baseado em certificados digitais, requer

uma infraestrutura de chaves públicas (ICP) para gerenciar os certificados para os usuários da rede *wireless*.”.

Este protocolo oferece autenticação mútua por meio da troca de certificados. Para sua autenticação e validação, o usuário deve enviar um certificado digital para o servidor, e o servidor de autenticação também deve fornecer um certificado. Quando é feito o processo de validação do servidor contra uma lista de autoridades de certificação confiáveis, o cliente terá uma maior segurança sobre quem estará conectado a uma rede autorizada. (GAST, 2005)

2.1.2.6 EAP - TTLS

O protocolo EAP-TTLS (*Extensible Authentication Protocol Tunneled Transport Layer Security*) se assemelha ao protocolo EAP-TLS, porém o certificado somente é instalado no servidor o que permite a autenticação do servidor por parte do cliente. A autenticação por parte do servidor se faz necessário o uso de métodos como nome do usuário/PW, CHAP (*Challenge Handshake Authentication Protocol*) e MSCHAPv2 (*Microsoft Challenge Handshake Authentication Protocol*). Com isso, o cliente não requisita um certificado digital, pois apenas o servidor de autenticação precisa de um, tornando o gerenciamento de credenciais do cliente simplificada (SANKAR et al., 2004)

2.1.2.7 EAP - FAST

O Flexible Authentication via Secure Tunneling (EAP-FAST) difere-se por apresentar uma autenticação respectiva estabelecida por meio de uma PAC (*Protected Access Credentials*), fornecida para o cliente de forma manual ou automática, no lugar de um certificado do servidor. Esse modelo de autenticação faz uso de sua capacidade de juntar autenticações múltiplas com o intuito de ligá-las criptograficamente. (INTEL, 2017)

2.1.2.8 PEAP

Protected Extensible Authentication Protocol (PEAP) é um modelo oriundo da 802.1x para WLANs, com a função de prover uma segurança adicional criando um canal TLS (*Transport Layer Security*) que ao obter êxito na autenticação do computador com *Network Policy Server* (NPS), que permite o desenvolvimento de diretivas de acesso e faz o gerenciamento central de autorizações, autenticações e de integridade do sistema, gera uma chave utilizada para criptografar todas as comunicações seguintes. O PEAP também possui alta extensão de banco de dados e suporte para autenticação e troca de senhas. Ele também pode ser utilizado em redes que fazem uso de mecanismos de proteção WPA e WPA2. (MICROSOFT, 200-?).

Como benefício cita-se a não vulnerabilidade a *dictionary attacks*, uma técnica de quebra de criptografia, a não exposição de *usernames* (nome de usuário) na resposta de identidade EAP, provê uma proteção dinâmica quando implantado em conjunto com TKIP e AES, entre outras funcionalidades.

Um processo seguro PEAP, é construído a partir de um canal TLS entre o PEAP e o NPS (*Network Policy Server*). Inicialmente o cliente é associado a um AP configurado como um cliente RADIUS para um servidor executor de NPS. Uma autenticação fornecida pelo IEEE 802.11 é feita como chave compartilhada ou sistema aberto antes da associação segura entre o cliente PEAP e AP. Se ocorrer êxito da associação, uma sessão TLS é negociada com o AP. Uma chave derivada é utilizada para criptografar as comunicações subsequentes do processo, o que inclui a autenticação de acesso à rede.

Para a obtenção de uma comunicação autenticada por EAP, deve-se estender o processo acima. Após o canal TLS ser criado entre o servidor NPS e entre o cliente PEAP, as credenciais do cliente tem a obrigação de serem informadas ao servidor NPS pelo canal criptografado. O AP encaminha as mensagens entre os clientes sem fio e o servidor RADIUS, não existindo a possibilidade de descriptografia por parte de Ponto de Acesso. Por fim, o servidor NPS deve fazer uma autenticação de usuário e computador cliente com o devido método de autenticação selecionado para o uso em

conjunto com o PEAP. Tal método pode ser por cartão inteligente ou senha de segurança, ou seja, EAP-TLS ou EAP-MSCHAPv2 respectivamente. (MICROSOFT, 200-?)

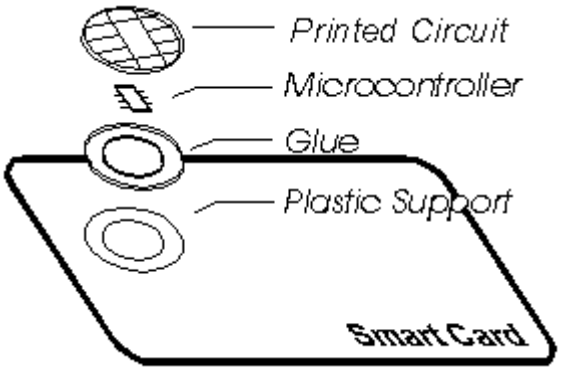
2.1.2.9 OUTROS MÉTODOS DE AUTENTICAÇÃO

Métodos de autenticação são vastos e além dos já citados, existem diversos outros, como cartões de segurança usados como *Tokens*, que geralmente possuem tamanhos e formas de cartões de créditos padrões. Estes podem exibir atributos distintos entre si, como em cartões bancários padrões, a utilização de um código de barras magnético, memória eletrônica interna em cartões de memória ou no caso de *Smart token*, até mesmo um micro controlador em seu interior.

Os cartões de memória geralmente são usados sozinhos de forma que para a "(...) autenticação do usuário, tais cartões são usados normalmente com algum tipo de senha ou número de identificação pessoal (*Personal Identification Number* — PIN). Uma aplicação típica é o caixa eletrônico (*Automatic Teller Machine* — ATM)." (Stallings e Brown 2015). A existência da senha aliada ao cartão aumenta a segurança, já que em caso de perda ou duplicação do mesmo, ainda existirá o número PIN para protegê-lo.

Os *Smart Tokens* são dispositivos portáteis que geram operações para seus usuários, geralmente identificando-o em um sistema mais robusto. O *Smart token* mais conhecido é o *Smart card*, conhecido também como cartão com chip e ele difere dos cartões de memória, por possuir um chip ou micro controlador em contato com um circuito impresso dentro de sua estrutura, como pode ser visto na Figura 5.

Figura 5: Estrutura Cartão Smart



Fonte: Grupo de Teleinformática e Automação da UFRJ[5]

Atualmente podem-se encontrar também dispositivos que fazem autenticação Biométrica através de características físicas, utilizando-as para reconhecimento de padrões. Segundo Stallings e Brown (2015), os modelos mais comuns de autenticação biométrica são: características faciais, impressões digitais, geometria da mão, padrão de retina, íris, assinatura e voz. Pode-se afirmar que em comparação a utilização de *tokens*, este método é complexo e caro.

Métodos de autenticação com *tokens* ou biometria são inovadores e aparentemente transmitem segurança aos seus usuários. Entretanto apesar de serem opções interessantes, ainda não encontramos seu uso dentro do âmbito educacional brasileiro.

2.2 SISTEMAS EMBARCADOS ABERTOS PARA ACCESS POINT

Ao comprar um *Access Point*, o usuário conta com um firmware padrão de fábrica na qual muitas vezes possuem limitações, interferindo no seu potencial. Para resolver esse problema, existem diversos projetos de código aberto que torna possível utilizar firmwares não oficiais e melhorar o desempenho do *Access Point*, explorando funcionalidades que não foram oferecidas pelo próprio aparelho. (HOLMES, 2016). Esses sistemas embarcados são suportados por vários fabricantes como TP-Link, D-

[5] Disponível em: https://www.gta.ufrj.br/grad/01_2/smartcard/smartcard.html

Link, CISCO e podem ampliar o alcance de sinal wireless do *Access Point* em alguns casos.

2.2.1 OPENWRT

O OpenWrt é um sistema embarcado muito adequado para dispositivos incorporados, com ênfase em *Access Point* sem fio. Diferente de muitos outros dispositivos na qual faz outras distribuições para os *Access Points*, o OpenWRT foi desenvolvido com o objetivo de ser um sistema operacional completo e de fácil alteraçã.(OPENWRT, 2017)

O OpenWrt permite uma grande personalização e flexibilização de dispositivos, então existe a possibilidade de utilizar diversos pacotes de componentes que atenda a necessidade de acordo com cada usuário na construção de uma aplicação. Com isso, esta distribuição torna-se uma das favoritas para os desenvolvedores de redes na qual possuem algum tipo de aplicação específica ou que necessita de protocolos customizados para o gerenciamento de rede.(SANTOS, 2011)

Entre as principais vantagens no uso do OpenWrt, está na distribuição da ferramenta opkg (*open package management*), que é um leve sistema de gerenciamento de pacotes, escrito na linguagem de programação C e apresenta uma variedade de arquivos mantidos em um repositório de pacotes locais ou pacotes disponibilizados na internet e oferecido pelos projetos OpenEmbedded e OpenWRT que por sua vez, propicia uma maior facilidade nas atualizações são disponibilizados para a plataforma.(NICKEL; BESSA, 2010)

Esse Firmware suporta vários mecanismos de segurança conforme a tabela 1.

Tabela 1: Mecanismos de proteção suportados

Segurança
WEP 64/128bit *WPA/WPA2.PSK* • Com servidor RADIUS ou chave compartilhada • Criptografia Unicast : AES/TKIP Filtragem de endereço MAC/Limitado

Fonte: WizFi630A Datasheet(2007), traduzida pelos autores.[6]

[6] Adaptado de: https://wiki.openwrt.org/_media/media/wiznet/wizfi630a_datasheet_en_v1_2_.pdf

Para saber se o equipamento de rede suporta o openwrt, é necessário fazer uma consulta na tabela de hardware do site do firmware, utilizando a marca e modelo do *access point*. No entanto, alguns equipamentos não estão cadastrados na tabela de hardware, então será estimado um hardware mínimo que suporte o OPENWRT baseado nas menores configurações de *Access Points* encontradas no site.

Hardware mínimo:

Memória RAM = 16MB/s, Memória FLASH = 4MB/s.

2.2.2 DD-WRT

O DD-WRT é outro sistema embarcado baseado em Linux de código aberto adequado a uma grande variedade de *Access Point*s WLAN e sistemas incorporados. O destaque principal está em prover um tratamento de grande facilidade e também favorecer o hardware utilizado com um amplo número de funcionalidades (REDE, 2011). Segundo Nickel e Bessa (2010), a mesma vem com uma interface gráfica instalada e operada pelo navegador em que pode ser facilmente configurada. Nickel e Bessa (2010) ainda reforça que o sistema DD-WRT foi desenvolvido com foco no desempenho (velocidade e estabilidade) aliado a adição de recursos não suportados pela versão original do firmware do fabricante do *Access Point*.

O DD-WRT é uma ferramenta muito utilizada e para sua utilização para fins privados, tal sistema está disponível gratuitamente. Caso seja necessária uma estrutura com redes de maior poder e confiabilidade (fins comerciais), a plataforma exige uma licença paga, permitindo configurar parâmetros da WLAN entre outras opções. (ABOUT... 2017)

Existe uma versão mínima (micro) que é programado apenas para funcionalidades básicas e a versão recomendada para adicionar pacotes de softwares adicionais. A versão micro é uma versão limitada, ajustada para caber apenas na memória flash mínima de 2MB de *Access Points* mais fracos baseados em Broadcom,

e 4MB de memória flash para o restante das plataformas (Atheros, Ralink, etc). Nesta versão, o usuário não será capaz de adicionar pacotes de softwares adicionais, porém já garante mais funcionalidades que o firmware padrão da maioria dos *Access Points*. A versão mínima recomendada para utilizar pacotes adicionais requisita 8 MB de memória flash.

Vale ressaltar que tanto o OPENWRT quanto o DD-WRT possuem uma tabela de hardware no próprio site e uma das marcas que mais suportam tal sistema é o TP-Link, *Access Point* que será utilizada para substituir alguns equipamentos nas escolas. (SUPPORTED… 2017)

2.3 EXPERIMENTAÇÃO REMOTA

Com a popularização e democratização da internet dentro das instituições de ensino, surge naturalmente um novo cenário: Técnicas didático-pedagógicas que pudessem fazer uso das Tecnologias da Informação e Comunicação. Desde meados dos anos noventa, as universidades brasileiras mantinham acesso à internet via RNP (Rede nacional de Pesquisa), entretanto, existia uma carência de conhecimento e abstração para que ocorresse algum progresso na utilização de tecnologias da informação naquela forma.

Silva (2006) define que um experimento remoto é criado quando os elementos que o compõem são reais. A ideia que se tem é que com uma interface virtual, aqueles que utilizam a aplicação possam ter as experiências que um laboratório normal proporciona, porém sem necessidade de estar fisicamente em um laboratório real.

Para entender o que é experimentação remota deve-se primeiramente conceituar as práticas de acesso remoto. O acesso remoto é uma tecnologia utilizada para obter acesso a um dispositivo não conectado fisicamente à rede retirando a necessidade que pessoas e hardware estejam de fato próximos. Então podemos dizer que experimentação remota, são técnicas e práticas feitas, utilizando a tecnologia de acesso remoto.

> Um laboratório de experimentação remota pode ser uma potente ferramenta que possibilite abrir os laboratórios aos alunos e a sociedade criando espaços

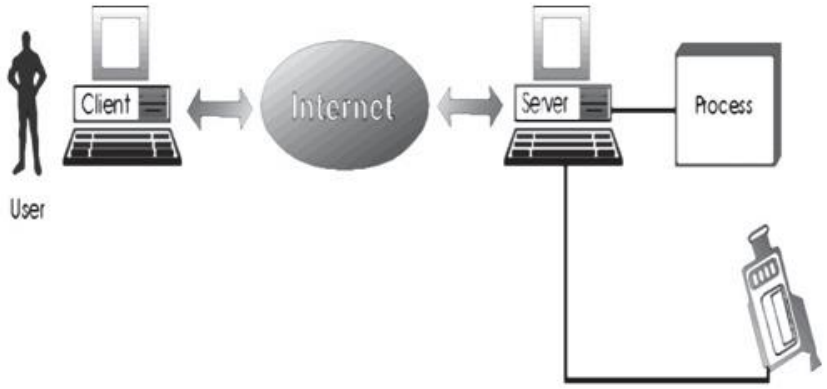
> virtuais orientados a geração, experimentação, descobrimento e transmissão de conhecimentos. (SILVA, 2006, p.122).

O Brasil possui um histórico extenso nas práticas de experimentação remota, na década de noventa professores da Universidade Federal de Santa Catarina especificamente da linha de pesquisas de Sistemas de Computação reuniram-se para desenvolver o laboratório de computadores, protocolo TCP/IP, Eletrônica Analógica, Eletrônica Digital e Sistemas de controle. Ao trazer especialistas das áreas citadas, estudou-se mais as possibilidades criando-se uma proposta denominado de Projeto Piloto de Experimentação Remota.

> O cliente acessa uma página, criada especificamente para este fim, onde pode manipular a distância o processo. Caso haja necessidade, uma câmera pode ser acoplada para que o cliente consiga visualizar o processo sendo monitorado e/ ou controlado. Toda a comunicação entre cliente e processo é feita através da Internet. (SILVA; FISCHER; ALVES, 2010, p.2)

O Projeto Piloto de Experimentação Remota consiste em um modelo semelhante a experimentação remota (ER) atual, no qual foi possível desenvolver um processo monitorado e controlado através da web como demonstrado na Figura 6.

Figura 6: Arquitetura do projeto piloto



Fonte: Experimentação Remota em Santa Catarina (SILVA, FISHER e ALVES, 2010)[7]

[7] https://periodicos.ifsc.edu.br/index.php/rtc/article/view/213

Segundo Silva, Fischer e Alves (2010) utilizou-se para o projeto piloto um micro controlador da Intel de arquitetura 8051 programável em linguagem de máquina Assembly com a funcionalidade 24/7 (vinte e quatro horas por dia e sete dias por semana).

Após o amadurecimento da ideia, desenvolveu-se uma linha de pesquisa dentro da Universidade Federal de Santa Catarina, especificamente no programa de pós-graduação em Ciência da Computação. Desta linha de pesquisa, surgiu um Micro Servidor Web (MSW), com a proposta de atuar como um servidor padrão, de tamanho e gasto reduzidos. “O projeto e desenvolvimento do MSW foi resultado de uma constatação: toda ER deveria ter seu servidor WEB customizado.”(SILVA; FISCHER; ALVES, 2010)

Com o sucesso, foi natural que novos projetos fossem elaborados, como o Projeto RExNet-Yippee - *Remote Experimentation Network - Yielding an Inter-University Peer-to-Peer e-Service*, que durante seus dois anos envolveu dez universidades e seis países.

> Portugal – Instituto Politécnico do Porto e Universidade do Porto, Alemanha – Universidade Técnica de Berlim e Universidade de Bremen, e Escócia – Universidade de Dundee; e 3 da América Latina: Brasil – Universidade Federal de Santa Catarina e Universidade Federal do Rio Grande do Sul, Chile _ Pontifícia Universidade Católica do Chile e Universidade Católica de Temuco; e México: Universidade de Monterrey.(SILVA; FISCHER; ALVES, 2010)

O projeto RExnet-Yippee obteve sucesso e possibilitou uma descentralização e ampliação da rede de relacionamento de pesquisadores na área. “Vale ressaltar que ER´s foram executados em todas as instituições do consórcio RExNet com resultados animadores para o futuro dos ER´s e suas aplicações” (SILVA; FISCHER; ALVES, 2010)

Um exemplo mais tangível obtido com o uso de ER foi a criação de um silo para armazenamento de grãos, na cidade de Araranguá, SC, Brasil hospedado pela Universidade do Sul de Santa Catarina - Unisul. Tal silo possuía 2,5 metros de altura e o mesmo de diâmetro com todas as funcionalidades normais do padrão e com ele foi executada ER a partir da cidade de Porto, Portugal, monitorando funções a partir do painel apresentado na Figura 7.

Figura 7: Página de acesso e controle do silo via ER

Fonte: Experimentação remota em Santa Catarina[8]

Atualmente na cidade de Araranguá, está em atividade o Rexlab, que desde 1997 vem executando com excelência diversos projetos educacionais no âmbito de ER. Entre eles pode-se destacar a utilização a utilização de Experimentação Remota em dispositivos móveis para a educação, que trouxe para as escolas públicas uma maneira diferente de ensino aliada à tecnologia. Em seus 20 anos de existência, o Rexlab, incentivou e popularizou conhecimentos científicos e tecnológicos, buscando sempre promover atualização e evolução do ensino com ênfase a ações e tecnologias remotas.

A experimentação remota tem uma necessidade eminente de profissionais multidisciplinares no que tange às diversas áreas de pesquisa, como direito, saúde e educação. Nesta última, por exemplo, exige-se uma participação efetiva da área pedagógica, capaz de identificar os desafios e características necessárias para um uso pleno da tecnologia em sala de aula, diferenciando sua abordagem à medida que se trabalha com diferentes estágios educacionais.

[8] https://periodicos.ifsc.edu.br/index.php/rtc/article/view/213

2.3.1 EXPERIMENTAÇÃO REMOTA NAS ESCOLAS PÚBLICAS

Diversos fatores reforçam o uso da tecnologia remota nas salas de aula, fatores esses, que impactam diretamente no ensino dos alunos. Dentre os problemas que existem nas escolas públicas, podemos citar a falta de laboratórios aplicados às disciplinas. Segundo o censo escolar do INEP (2013), estima se que cerca de 56% das escolas públicas brasileiras não possuem um laboratório de informática, tornando a possibilidade de utilização de softwares de ensino inexistente e mesmo as que possuem computadores, não os tem em quantidade suficiente (ROCHADEL et al., 2016). Além dessa falta de equipamentos, essas mesmas escolas, não contam com uma distribuição de sinal wireless eficiente, isso quando possuem alguma. Esses fatores estruturais não são os únicos problemas encontrados, a educação no Brasil ainda sofre com externalidades, como greves, paralisações e feriados.

> O primeiro limitante é o tempo de aula da Educação Básica. No Brasil, cada aula possui cerca de 50 minutos, que são considerados como uma hora aula. Estimando 200 dias letivos e em média três aulas semanais, são 120 horas aula por ano. Período muitas vezes prejudicado por feriados, paralisações e greves. (ROCHADEL et al., 2016, p.2)

Apesar dos empecilhos encontrados pela experimentação remota nas escolas, existem casos de sucesso. Motivados a superar os problemas, alguns projetos ultrapassaram as barreiras encontradas e conseguem cumprir seus objetivos.

Levando em conta que a atual geração de estudantes são nativos digitais, ou seja, nasceram com a tecnologia digital consolidada em suas vidas, deve-se valorizar tal característica e utilizá-la em favor do ensino. O uso de tecnologia na sala de aula, por si só já se faz interessante ao aluno, chamando sua atenção, diferente do ensino retrógrado e clássico. Ensino esse que envolve muita teoria e pouca prática, tornando inflexível o aprendizado, de modo que alunos se formam sem nunca terem feito um experimento real.

> Assim, ao tratar-se de novas formas de utilização das tecnologias, deve-se considerar a capacidade desta tecnologia de atrair o aluno e aproximá-lo dos conteúdos abordados. Por si só já são bastante atrativos os simuladores e laboratórios virtuais com experiências simuladas de resultados gravados; mas, além destes recursos, a utilização de recursos remotos tende a permitir uma experiência ainda mais real (SIMÃO et al, apud PALADINI, 2013, p.2).

É neste escopo, que a experimentação remota (RE) nas escolas entra, podendo aproximar os alunos das ciências naturais e exatas, dando a oportunidade de que exista no ensino algum tipo de experimento prático, apesar da inexistência de laboratórios, aproximando-o e despertando interesse no conteúdo abordado.

Um dos grandes pilares da experimentação remota (RE) nas escolas é com o uso de dispositivos móveis. Dispositivos móveis, se adaptam facilmente aos aspectos fundamentais para o uso tecnológico por Simão et al (2013). São fáceis de usar (Usabilidade), fáceis de transportar (Portabilidade), são eficientes (Funcionalidade), são acessíveis a grande parte da população (Acessibilidade) e conseguem ser encontrados em qualquer lugar (Ubiquidade). Esse conjunto de fatores torna os dispositivos móveis perfeitos para a sala de aula.

Para essa realidade criou-se programa InTecEdu, desenvolvido pelo Laboratório de Experimentação Remota (RExLab) da Universidade Federal de Santa Catarina (UFSC) e apoiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e Rede Nacional de Ensino e Pesquisa (RNP). O programa InTecEdu, visa a partir da integração de dispositivos móveis, prover acesso a conteúdos didáticos complementados no uso da tecnologia remota na interação com ambientes virtuais de aprendizagem, objetos de aprendizagem, simuladores e experimentos remotos. A partir desse programa diversos projetos foram submetidos e aprovados, entre eles está o *Promovendo a inclusão digital em escolas de Educação Básica da rede pública a partir da integração de tecnologias inovadoras de baixo custo no ensino de Ciências Naturais e Exatas*. Tal projeto, possibilita a compra de dispositivos indispensáveis para que as quatro escolas contempladas da microrregião de Araranguá possam usufruir com exito das praticas remotas.

3 DESENVOLVIMENTO

Este capítulo objetiva abordar sobre a infraestrutura de rede das escolas que participaram desta pesquisa e o gerenciamento de senha das mesmas, explicando qual tipo de autenticação de rede cada escola está utilizando atualmente e os protocolos de segurança utilizados nos *Access Points*.

3.1 INFRAESTRUTURA DE REDE NAS ESCOLAS

Foi coletado dados a respeito da infraestrutura de três escolas do município de Araranguá e uma escola do município de Balneário Arroio do Silva na qual fará parte dessa pesquisa para a aplicação das melhorias. Após a coleta de dados, elaborou-se uma lista dos equipamentos presentes nas escolas, com as informações de nome, modelo e localização. Ainda foi desenvolvido um mapa geral, identificando a qualidade do sinal de rede sem fio em cada sala e classificando a qualidade do sinal em quatro categorias : baixo sinal de wireless, bom sinal de wireless, ótimo sinal de wireless e sem sinal de wireless, apontando assim a localização dos *Access Points.* Foi identificado também, o gerenciamento aplicado nas escolas, de forma que fossem estudados para a futura melhora da segurança das redes sem fio.

As escolas participantes foram: Escola de Educação Básica Profº. Apolônio Ireno Cardoso - pertencente ao município de Balneário Arroio do Silva, Escola de Educação Básica Profª Maria Garcia Pessi, Escola de Educação Básica de Araranguá e a Escola de Educação Básica Profº Otávio Manoel Anastácio.

3.1.1 EEB PROFº APOLÔNIO IRENO CARDOSO

A Escola E.E.B Profº Apolônio Ireno Cardoso possui dois links de internet. Um switch fica na secretaria e o outro switch fica na sala de informática. Na secretaria a escola conta com um link de 4MB/s do CIASC (Centro de Informática e Automação de Santa Catarina) em que divide a internet para todos os computadores da secretaria e distribui o sinal por um *Access Point* no mesmo local. Na sala de informática possui

um link de 10MB/s de uma empresa contratada na região de Araranguá e divide esse link para o restante da escola.

A quantidade, modelo e local dos equipamentos de rede da escola estão detalhadas na tabela à seguir.

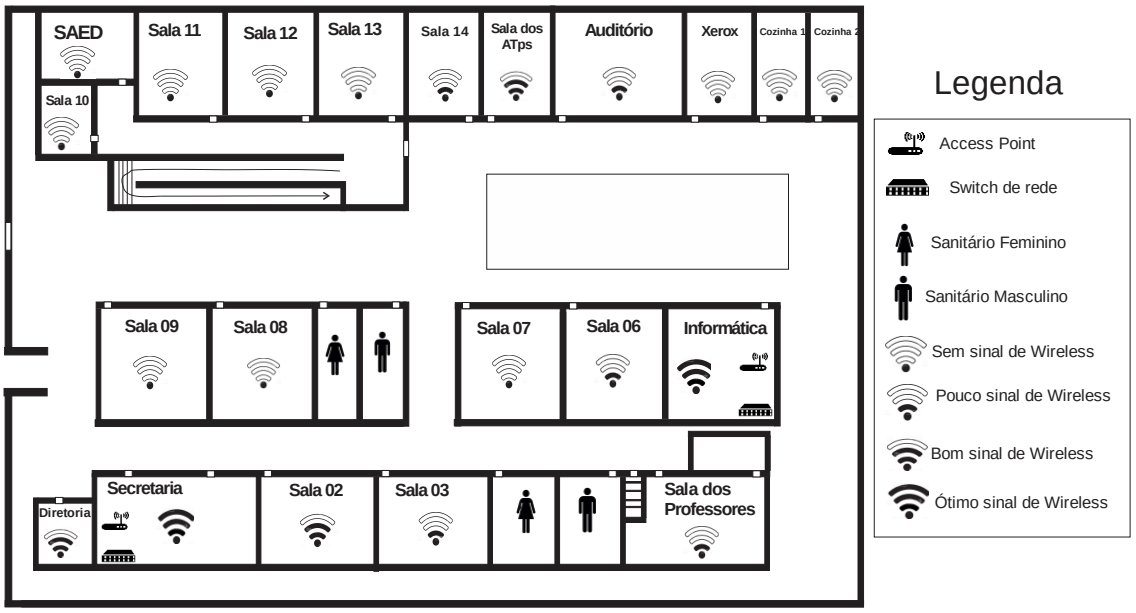
Tabela 2: Tabela de equipamentos da EEB Profº Apolônio Ireno Cardoso

Quantidade	**Equipamento**	**Modelo**	**Local**
01	*Access Point* TP-Link	WR740N	Informática
01	*Access Point* Intelbras	WAG20E	Informática
01	*Access Point* Intelbras	WRN240Slin	Secretaria
01	*Access Point* TP-Link	TL-WDL4300	1º Andar

Fonte: Elaborada pelos autores.

Entre os equipamentos de rede listados na tabela acima, o único que não está sendo utilizado é o *Access Point* Intelbras, modelo WAG20E e se encontra desligado na sala de informática. O *Access Point* que situa-se no 1º andar, está em funcionamento, porém, está distribuindo sinal sem internet, conforme figura 8.

Figura 8: Mapa do térreo da Escola de Educação Básica Profº Apolônio Ireno Cardoso



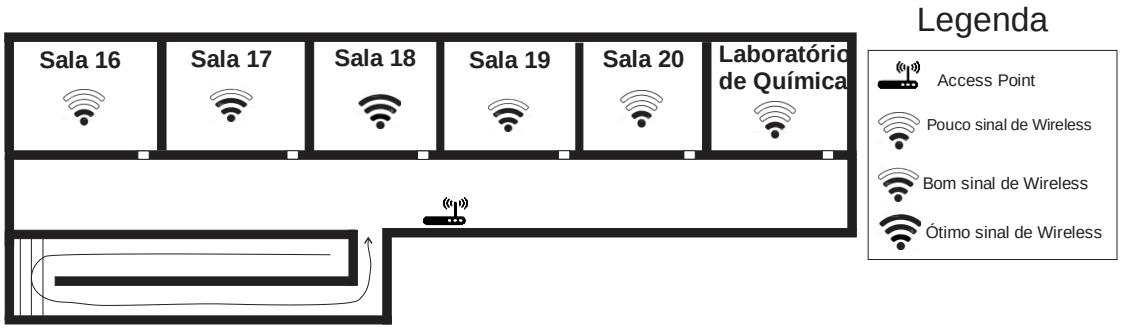
Fonte: Elaborada pelos autores.

Conforme a figura mostra, nota-se uma baixa qualidade de sinal em quase todos os pontos da escola, até mesmo nas salas que estão ao lado ou muito próximos de algum ponto de acesso. Isso acontece pelo fato da estrutura escolar possuir paredes grossas, interferindo na distribuição de sinal de internet, mal posicionamento dos *Access Points* ou até mesmo má qualidade dos mesmos.

Qualidade do sinal de Wireless:

- **Ótimo sinal de Wireless:** As salas em que possuem um sinal de ótima qualidade estão aquelas em que dispõem de pontos de acessos, como a secretaria e informática.
- **Bom sinal de Wireless:** As salas que mantiveram um bom sinal mesmo não tendo um ponto de acesso no mesmo local, são a sala 02 e a sala da assitência técnica pedagógica (ATP), uma fica ao lado de uma sala que possui ponto de acesso e a outra capta sinal do *Access Point* que está no 1º andar.
- **Baixo sinal de Wireless:** As salas em que ficaram com sinal baixo estão: sala dos professores, sala 03, sala 06, sala 13 e sala 14,
- **Sem sinal de Wireless:** Os restantes das salas estão sem internet, são elas: SAED, sala 07, 08, 09, 10, 11, 12, auditório e Xerox.

Figura 9: Mapa do 1º andar da Escola de Educação Básica Profº Apolônio Ireno Cardoso



Fonte: Elaborada pelos autores.

No primeiro andar da escola estão as salas do ensino médio, em que se encontra o *Access Point* TP-Link, modelo TL-WDL4300 no corredor, responsável pela distribuição de sinal para todas as salas deste andar, porém, sem internet.

Qualidade do sinal de Wireless:

- **Ótimo sinal de Wireless:** A sala que mantêm um ótimo sinal é a que está em frente ao Access Point (sala 18) conforme mostra a figura 9.
- **Bom sinal de Wireless:** As salas 17 e 19 estão com um bom sinal
- **Baixo sinal de Wireless:** As salas 16, 20 e laboratório de química mantém uma baixa qualidade de sinal *wireless.*

3.1.1.1 GERENCIAMENTO DE SENHAS E SEGURANÇA NO EEB PROFº APOLÔNIO IRENO CARDOSO

Atualmente na escola de ensino básico profº Apolônio Ireno Cardoso, não existe nenhum profissional que faça a troca e gerenciamento das senhas, até mesmo poucos professores conhecem a senha *wifi*. Para utilizar dispositivos móveis nas práticas pedagógicas e utilização de experimentos remotos os alunos devem ser deslocados para a sala de informática, sendo o único local que possui um sinal de rede estável. Já para fazer a conexão de rede sem fio desses alunos, é necessário que o tutor que estiver coordenando a atividade conheça a senha de acesso ao *wifi,* passando essa senha para todos os aluno. Todavia, ao utilizar mais de vinte dispositivos conectados, ocorre uma sobrecarga de rede, acarretando em perdas de estabilidade tornando as práticas remotas difíceis de serem executadas.

Dos três *Access Points* pertencentes à escola, os localizados na secretaria e no primeiro andar fazem uso dos protocolos de proteção de rede WPA/WPA2, que nada mais é do que um modo misto entre os protocolos de segurança WPA e WPA2. Esse modo atua de forma que permite tanto dispositivos novos quanto os mais antigos possam utilizar a rede. Ou seja, enquanto os novos fazem uso da criptografia AES, os antigos utilizam criptografia TKIP. Já o localizado na informática, utiliza protocolo WPA2-PSK (*Pre-shared key*) que possui uma chave pré compartilhada E sua criptografia é a AES (Padrão de Criptografia Avançada), um padrão muito utilizado em redes domésticas.

3.1.2 EEB PROFª MARIA GARCIA PESSI

A Escola E.E.B Profº Maria Garcia Pessi, possui dois links de internet e entre as quatro escolas relatadas, é a que apresenta a menor estrutura de rede e precisa o maior trabalho para obtenção de bons resultados. Um link de internet encontra-se na secretaria, com banda larga de 2MB/s do CIASC, em que distribui a rede para secretaria, biblioteca e sala dos professores. O outro link de internet está na sala de informática com banda larga de 5MB/s de uma empresa contratada na região, distribuindo sinal wireless para o restante da escola.

Os equipamentos de rede da escola estão descritos na tabela 3.

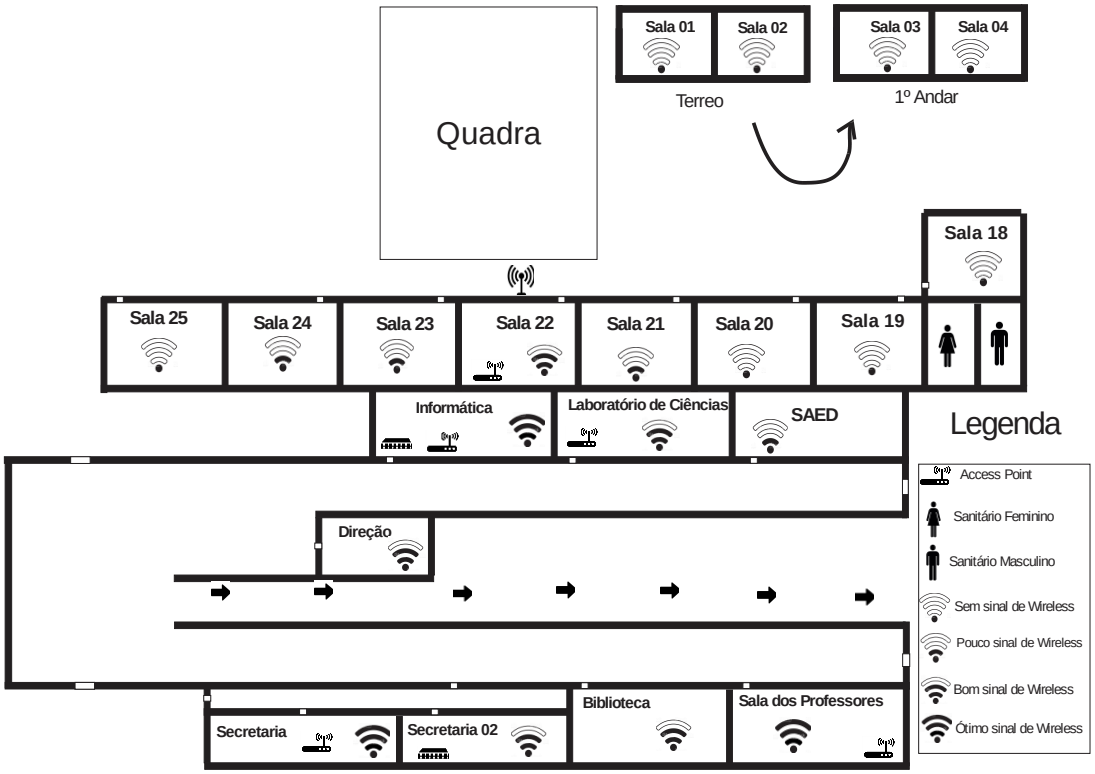
Tabela 3 : Equipamentos encontrados na EBB Maria Garcia Pessi

Quantidade	**Equipamento**	**Modelo**	**Local**
01	Antena	Omni 12DBI MM2412 Aquário	Telhado (sala22)
01	*Access Point* TP-Link	TL-WR750N	Informática
01	*Access Point* TP-Link	TL-WR750N	Lab.Ciências
01	*Access Point* TP-Link	TL-WR750N	Secretaria
01	*Access Point* Multilaser	Re171	Sala. Professores
01	*Access Point* Intelbras	WRN240	1ºAndar
01	*Access Point* Intelbras	Win240	Sala 22

Fonte: Elaborada pelos autores.

Esses equipamentos estão distribuídos conforme a figura 10.

Figura 10: Mapa do térreo da Escola de Educação Básica Profº Maria Garcia Pessi



Fonte: Elaborada pelos autores.

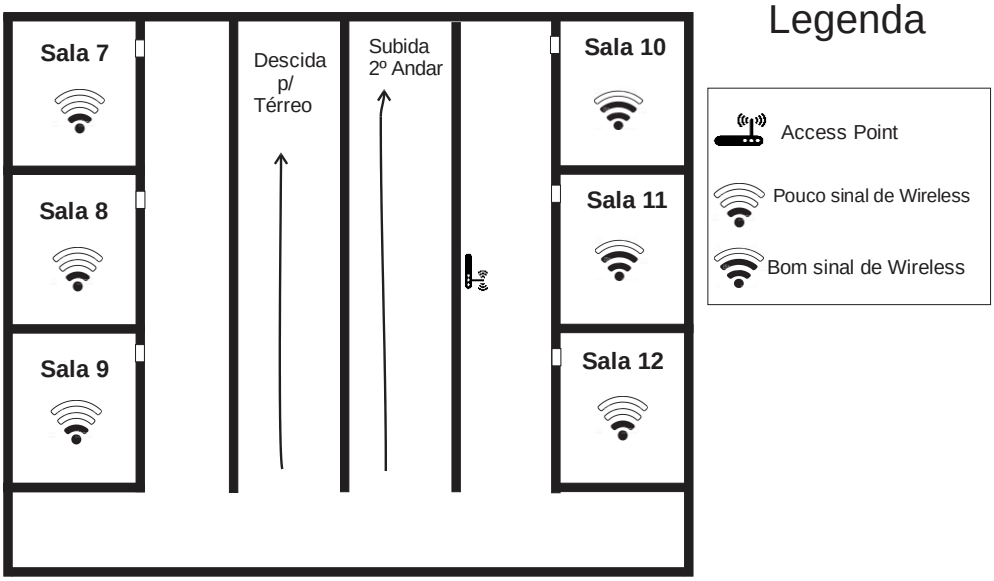
Qualidade de sinal de wireless :

- **Ótimo sinal de wireless:** Algumas salas mantêm uma ótima qualidade de sinal wireless como, por exemplo, Secretaria, sala dos professores e Informática. Todas essas salas possuem um *access point* no local;
- **Bom sinal de wireless:** A secretaria 02, biblioteca, direção, laboratório de ciências e sala 22 conseguem atingir um bom sinal de wireless.
- **Baixo sinal de wireless:** O laboratório de ciências, SAED, sala 21, 23 e 24 estão com baixo sinal;
- **Sem sinal de wireless:** As salas 18, 19, 20, 25 e as salas do prédio que ficam do lado direito da quadra que é o térreo e 1º andar (salas 1, 2, 3 e 4) estão atualmente sem sinal wireless.

Um detalhe importante é que a escola possui um *access point* Intelbras modelo win240 na sala 22 em que compartilha sinal para uma antena wireless que está no

telhado com o objetivo de espalhar o sinal wireless para o prédio logo a frente ao lado da quadra (sala 1,2,3 e 4), porém é necessário melhorar o alcance desse sinal.

Figura 11: Mapa do 1º andar da Escola de Educação Básica Profº Maria Garcia Pessi



Fonte: Elaborada pelos autores.

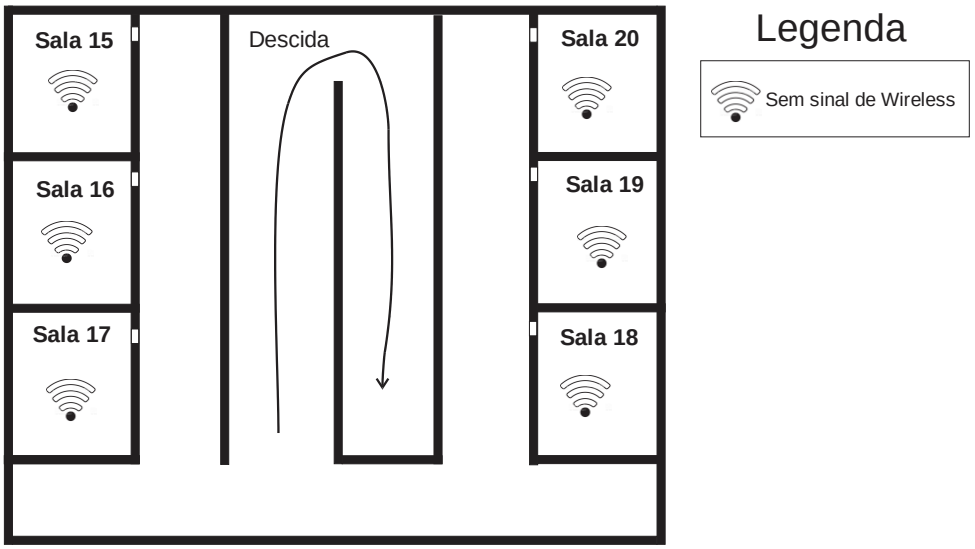
No primeiro andar encontra-se o *Access Point* Intelbras modelo WRN 240 em frente a sala 11, mas, está desligado e os sinais das respectivas salas de aula estão com sinal dos AP´s (*Access Point*) do andar de baixo (Térreo).

Qualidade de sinal *wireless*:

- **Bom sinal de Wireless:** As salas 10 e 11 estão com um bom sinal
- **Baixo sinal de wireless:** As salas 7, 8, 9 e 12 estão com baixo sinal.

No segundo andar todas as salas estão sem sinal wireless conforme descreve na Figura 12.

Figura 12: Mapa do 2º andar da Escola de Educação Básica Profº Maria Garcia Pessi



Fonte: Elaborada pelos autores.

- **Sem sinal de wireless** : todas as salas (salas 15, 16, 17, 18, 19 e 20)

3.1.2.1 GERENCIAMENTO DE SENHAS E SEGURANÇA NA EEB PROFª MARIA GARCIA PESSI

A escola de educação básica Profª Maria Garcia Pessi, possui um gerenciamento de senhas feito por somente uma professora, que faz a troca de senhas quando necessário. Dentro da instituição ninguém mais sabe como modificar a senha dos *Access Points*.

Para a utilização da tecnologia em práticas pedagógicas, é necessário que os alunos se locomovam para a sala de informática e não é atípico os tutores trazerem um *Access Point* para definir uma senha de acesso para os alunos, pois muitos desconhecem da senha que pertence ao *Access Point* do local. Desse modo, é definido uma senha para o novo *Access Point* que é passado para os alunos. Vale ressaltar que a escola apresenta um link de apenas 5 MB/s para essas aplicações.

Dos *Access Points* pertencentes à escola, dois deles mantêm protocolos WPA/WPA2, são os encontrados no LabCiencias e nas salas dos professores, promovendo conexão a dispositivos novos e antigos. Os outros três, pertencentes a informática, sala 22 e secretaria, utilizam do WPA2 *Personal*, com criptografia AES.

3.1.3 EEB DE ARARANGUÁ

A Escola de Educação Básica de Araranguá é a escola em que possui a melhor distribuição de sinal wireless entre as quatro pesquisadas. A escola conta com quatro *Access Points* Intelbras modelo WRN240i que são distribuídos entre a secretaria e os corredores das salas (térreo e 1º andar) e um *Access Point* D-Link que é localizado na sala de informática. A escola possui dois links de internet, uma de 2 MB/s do CIASC na sala de informática e um link de 15 MB/s localizado na sala da direção. O Link de 2 MB/s é dividido para os computadores da sala de informática e um *Access Point* D-Link. O link de 15 MB/s é distribuído para o restante da escola.

Embora a escola possua uma boa estrutura de rede wireless (figura 12 e 13), a mesma relata problemas em relação à velocidade de banda, já que toda a estrutura da escola é alimentada por uma rede de 15MB/s, perdendo muito desempenho nos dias em que várias salas precisem utilizar a internet para alguma atividade em aula.

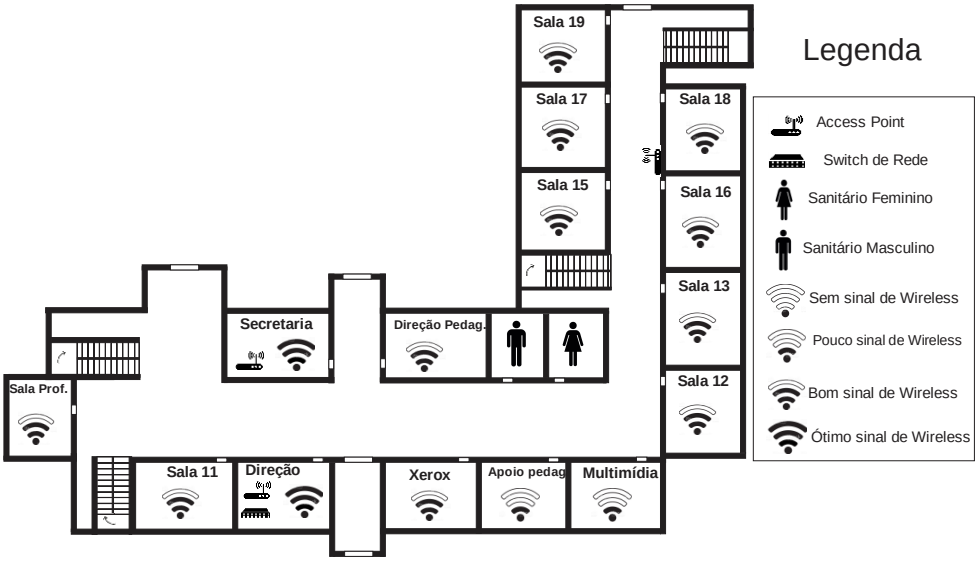
Tabela 4 : Lista de equipamentos da EBB de Araranguá

Quantidade	**Equipamento**	**Modelo**	**Local**
01	*Access Point* D-Link	DI524	Informática
01	*Access Point* Intelbras	WRN240 Slin	Secretaria
01	*Access Point* Intelbras	WRN240I	Direção
01	Roteador Mikrotik	750	Direção
01	*Access Point* Intelbras	WRN240I	Corredor Térreo
02	*Access Point* Intelbras	WRN240I	1º Andar, corredor

Fonte: Elaborada pelos autores.

Os equipamentos estão distribuídos em toda a estrutura da escola conforme as figuras 13 e 14 a seguir.

Figura 13: Mapa do térreo da Escola E.E.B de Araranguá



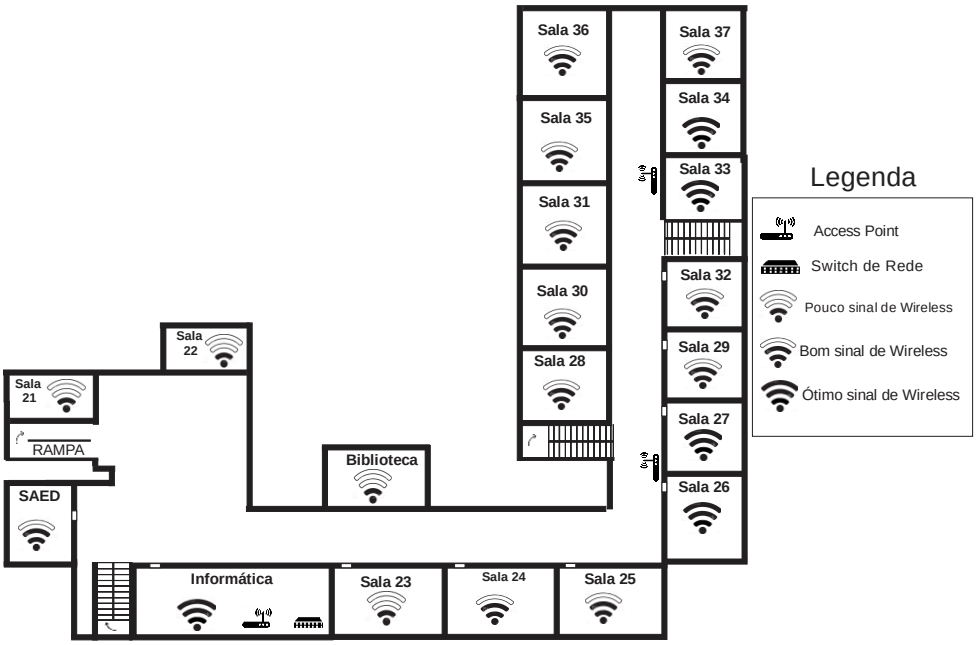
Fonte: Elaborada pelos autores.

Qualidade de sinal de wireless:

- **Ótimo sinal de wireless :** direção e secretaria
- **Bom sinal de wireless :** A maioria das salas contam com um bom sinal de wireless como : sala dos professores, sala 11, direção pedagógica, xerox, salas 12, 13, 15, 16, 17, 18 e 19.
- **Baixo sinal de wireless :** Apoio pedagógico e sala de multimídia.

Conforme demonstra o mapa geral do térreo da escola E.E.B de Araranguá, as únicas salas que contam com um baixo sinal de wireless são as salas apoio pedagógico e multimídia. Os restantes das salas estão com bom ou ótimo sinal de wireless.

Figura 14: Mapa do 1º andar da escola E.E.B de Araranguá



Fonte: Elaborada pelos autores.

Aqui a distribuição de sinal wireless é bem parecida com a do térreo exceto por um detalhe: As salas 21,22, 23 e biblioteca estão com pouco sinal de wireless, enquanto os restantes estão com bom ou ótimo sinal de wireless.

Qualidade de sinal wireless:

- **Ótimo sinal de wireless:** Informática, salas 26, 27, 33 e 34.
- **Bom sinal de wireless:** SAED, salas 24 e 25
- **Baixo sinal de wireless:** Biblioteca, salas 21, 22 e 23.

3.1.3.1 GERENCIAMENTO DE SENHAS E SEGURANÇA NA EEB DE ARARANGUÁ

O gerenciamento de senhas da escola de ensino básico de Araranguá é feito exclusivamente por meio da empresa contratada para fornecer internet a instituição e quando solicitada, faz a mudança das senhas e resolve os problemas que ocorrerem. Não foi encontrado nenhum funcionário da escola permitido a fazer o gerenciamento das redes.

Antigamente a escola utilizava o roteador Mikrotik modelo 750 que gerenciava a rede sem fio por meio dos endereços MAC, permitindo acesso exclusivo à dispositivos cadastrados. No entanto isso inviabilizava o acesso aos dispositivos móveis para as aplicações pedagógicas na escola, pois além de possuir uma limitação de equipamentos cadastrados, não existia um profissional capacitado para o gerenciamento do equipamento.

Entre as quatro escolas pesquisadas, a EEB de Araranguá é a única em que os professores precisam fazer uso da internet assim que entram na sala para fazer a chamada *online* dos alunos. Então a escola conta com uma estrutura de rede bem estável em comparação com as outras escolas.

Atualmente a escola possui apenas uma senha para todos os *Access Points*, sem trocas periódicas, que é passada para os alunos durante as aplicações pedagógicas. Desse modo a rede de 15MB/s é sobrecarregada, pois os alunos conhecem a senha.

Existe cinco *Access Points* utilizados no local, deles somente um mantém o protocolo WPA/WPA2, servindo a dispositivos novos e antigos, este pode ser encontrado na secretaria. Os outros quatro, estão localizados um na direção, um no corredor no térreo e dois no primeiro andar, todos com o protocolo WPA2 *Personal*, com criptografia AES.

3.1.4 EEB PROFº OTÁVIO MANOEL ANASTÁCIO

A escola EEB Profº Otávio Manoel Anastácio possui três *Access Points*, sendo um utilizado como modem/roteador na secretaria e outros dois *Access Points* de baixa qualidade localizados na biblioteca e sala dos professores.

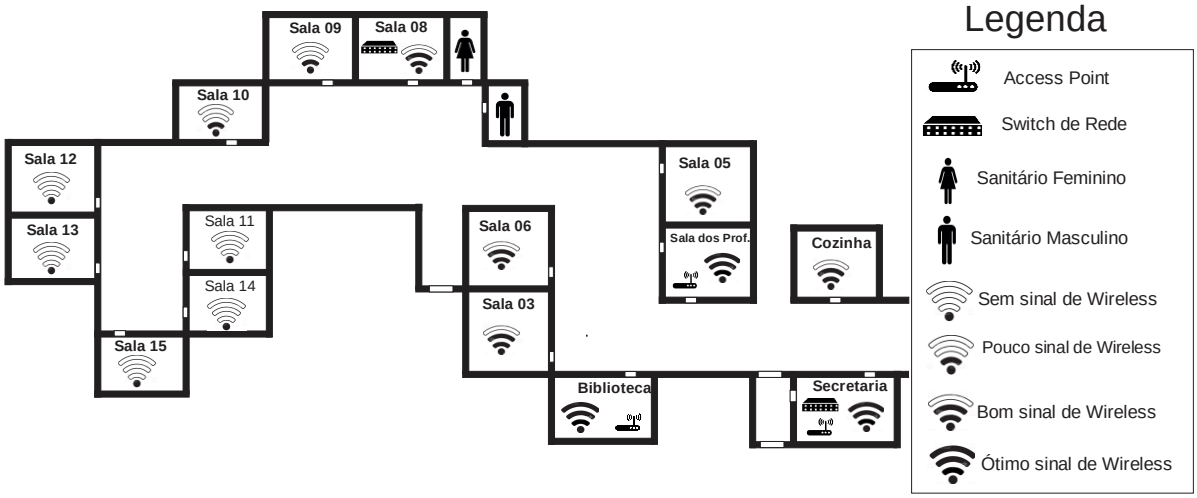
Tabela 5 : Lista de equipamentos do E.E.B Profº Otávio Manoel Anastácio

Quantidade	Equipamento	Modelo	Local
01	*Access Point* TP-Link	TD-8816	Secretaria
01	*Access Point* Kaiomy	APR-4PN	Sala.Prof.
01	*Access Point* Knup	KNUP-KP-R02	Biblioteca

Fonte: Elaborada pelos autores.

Sua estrutura conta com dois links de internet, um link do CIASC de 2 MB/s localizado na secretaria em que distribui para um *Access Point* na biblioteca e um modem/roteador na secretaria e um link de 8 MB/s na sala 08, distribuindo internet para um *Access Point* na sala dos professores conforme a Figura 15.

Figura 15: Mapa da E.E.B Profº Otávio Manoel Anastácio



Fonte: Elaborada pelos autores.

Qualidade de sinal wireless:

- **Ótimo sinal de wireless :** Secretaria e biblioteca.
- **Bom sinal de wireless** : Cozinha, salas 03, 05, 06 e 08.
- **Baixo sinal de wireless :** Salas 09 e 10.
- **Sem sinal de wireless :** Salas 11, 12, 13, 14 e 15.

3.1.4.1 GERENCIAMENTO DE SENHAS E SEGURANÇA EBB OTÁVIO MANOEL ANASTÁCIO

O gerenciamento de senhas encontrado na escola de Ensino Básico Profº Otávio Manoel Anastácio é feito exclusivamente pelos técnicos do Município de Araranguá, comparecendo somente quando a direção entra em contato com a prefeitura relatando problemas. Portanto, não existe nenhum profissional dentro da

escola para essa função, e os professores desconhecem sobre gerenciamento e segurança de rede.

Quando ocorre práticas pedagógicas com o uso de redes sem fio, os alunos localizados no lado esquerdo da escola, sala 09 à 15, são movidos para o lado oposto da escola, ou seja, para o local que possui uma melhor estabilidade de rede *wireless*, conforme demonstra a figura 15.

Para as aplicações pedagógicas, a senha dos *Access Points* é repassada para os alunos e não possuem uma troca de senha regular.

Os *Access Points* existentes na estrutura são mantindos com um senha padrão para todos, com somente números e letras, sem caracteres especiais. O protocolo de segurança utilizado é o WPA2-Personal com criptografia AES em todos os *Access Points*.

4 PROPOSTA

Neste capítulo são disponibilizadas as propostas elaboradas para um melhor funcionamento da infraestrutura de redes das escolas. Aqui, é demostrado quais equipamentos deverão ser substituídos e quais equipamentos serão adicionados para que ocorra uma unanimidade para o uso dos sistemas embarcados OPENWRT e DD-WRT. Além disso, as localizações novas focam-se na distribuição de sinal wireless por toda a área das escolas, possibilitando futuramente o uso de dispositivos para as práticas remotas. Não serão utilizados os *links* de acesso do CIASC (Centro de Informática e Automação de Santa Catarina), devido a eles serem exclusivamente para uso da secretaria.

Uma observação importante, é que alguns equipamentos foram adicionados nos corredores e outros não. Nos locais em que foram adicionados equipamentos dentro das salas, é devido a existência de uma estrutura aberta que pode colocar em risco os novos *Access Points* adicionados. Portanto, nestes locais foram necessários mais *Access Points*, já que a estrutura escolar possui paredes grossas e acontece uma grande perda de sinal de uma sala à outra. Nos locais em que foram adicionados *Access Points* nos corredores deve-se a estrutura ser fechada, diminuindo o risco de furtos e eventuais danos.

4.1 EQUIPAMENTOS DISPONIBILIZADOS PELO PROJETO

Com a verba do projeto *Promovendo a Inclusão Digital em Escolas de Educação Básica da Rede Pública a Partir da Integração de Tecnologias Inovadoras de Baixo Custo no Ensino de Ciências Naturais e Exatas*, serão disponibilizados equipamentos de rede que farão a reestruturação de redes sem fio nas escolas. Além dos equipamentos, será disponibilizado um link de 15 MB/s com intuito de solucionar, em conjunto com os equipamentos, os problemas encontrados nas escolas. A lista dos equipamentos encontra-se na tabela 6 abaixo.

Tabela 6 : Lista dos equipamentos novos adquiridos.

Quantidade	Equipamento	Modelo
10	*Access Point* TP-Link	TL-WR1043ND
01	*Access Point* TP-Link	TL-WR741ND
01	Servidor *Raspberry* pi	3
04	Roteador Balanceamento de Carga TP-Link	TL-R470P+

Fonte: Elaborada pelos autores

Os *Access Points* TP- Link modelo TL-WT1043ND e TL-WR741ND serão utilizados para proporcionar uma distribuição *wireless* de alta qualidade, mantendo protocolos de segurança com criptografia avançada, suportando os sistemas embarcados como OPENWRT e DDWRT para um melhor alcance de sinal *wireless*, além de um eficiente gerenciamento de senhas.

Os roteadores de balanceamento de carga TP-Link modelo TL-R470+ serão utilizados de forma de unificar o link existente da escola com o novo link de 15 MB/s disponibilizado pelo projeto, possibilitando uma gestão eficiente, coordenando – os e selecionando o link mais estável no momento do acesso.

Por último, um servidor *Raspberry* pi modelo 3 com um micro SD de 8Gb que ficará responsável pelo gerenciamento dos acessos aos *Access Points* de uma escola.

4.2 EEB PROFº APOLÔNIO IRENO CARDOSO

Conforme o mapa estrutural atual da escola nota-se um grande déficit de distribuição de sinal wireless encontrado no térreo, mesmo nos locais que estão próximos dos Access Points. Isso ocorre principalmente devido ao grande isolamento de sinal de wireless por conta de estrutura antiga da escola, possuindo paredes muito grossas, além de fatores como equipamentos defasados e mal posicionados.

A proposta para uma boa distribuição de sinal wireless para o térreo da instituição é feita inicialmente com o deslocamento de *Access Points* que serão reutilizados para a nova estrutura de rede da escola. Esses *Access Point* suportam firmwares como OPENWRT e DD-WRT que farão o gerenciamento de senhas através de *scripts*, além de aumentar o alcance de sinal de *wireless*.

Conforme a tabela 7, dois equipamentos da escola serão retirados, pois não possuem hardware suficiente para suportar os firmwares escolhidos.

Tabela 7: Equipamentos retirados de EEB Prof Apolônio Ireno Cardoso

Equipamento	**Modelo**	**Local**
Access Point Intelbras	WAG20E	Informática
Access Point Intelbras	WRN240Slin	Secretaria

Fonte: Elaborada pelos autores.

Os equipamentos escolhidos para serem adicionados na escola, são quatro TP-Links, sendo que três são *Access Points* e um é roteador de balanceamento de carga na sala de informática, na qual fará o junção e distribuição do link de 10MB/s atual e o link de 15MB/s que será adicionado posteriormente na escola, fazendo um balanceamento inteligente, proporcionando ao usuário a seleção da conexão mais eficiente. Os equipamentos adicionados podem ser vistos na tabela 8.

Tabela 8 : Equipamentos Adicionados à EEB Prof Apolônio Ireno Cardoso

Equipamento	**Modelo**	**Local**
Access Point TP-Link	TL-WR1043ND	Corredor, sala 02
Access Point TP-Link	TL-WR1043ND	Corredor, auditório
Access Point TP-Link	TL-WR1043ND	Corredor, sala 12
Roteador Balanceamento de carga TP-Link	TL-R470T+	Informática

Fonte: Elaborada pelos autores.

O plano de proposta da escola está detalhado na Figura 16.

Figura 16: Proposta para o térreo da EBB Apolônio Ireno Cardoso

Fonte: Elaborada pelos autores.

Para o térreo da instituição, será necessário adicionar um novo *Access Point* TP-link, modelo TL-WR1043ND que ficará localizado no corredor, em frente à sala 02, distribuindo o sinal wireless para a diretoria, secretaria e salas 02, 03, 08 e 09, que atualmente possuem um baixo sinal de wireless disponível. O *link* de internet localizado na secretaria pertencente a CIASC, será utilizado apenas para a estrutura de computadores localizado na própria secretaria, então será desligado o *Access Point* Intelbras modelo WRN240 Slim. Todos os *Access Point* da escola estarão conectados via *ethernet* ao acesso localizado na sala de informática.

O *Access Point* atual da informática será movido para o corredor em frente a sala dos professores, tornando mais eficiente a distribuição de sinal para a sala dos professores, salas 06, 07 e informática.

Outros dois novos *Access Points* serão adicionados, um deles ficará no corredor em frente a sala 12 e o outro em frente ao auditório, resolvendo a falta de sinal encontrada atualmente nestes locais.

Para o 1º Andar, não será acrescentado nenhum equipamento novo, somente é necessário uma atualização do firmware para que o *Access Point* TP-Link modelo TL-WDL4300 aumente o alcance de sinal wireless para as salas de baixo sinal.

4.3 EEB PROFª MARIA GARCIA PESSI

A escola EEB Profº Maria Garcia Pessi dispõe de alguns *Access Points* TP-Links que possuem configurações mínimas para suportar o OPENWRT e DD-WRT. Esses equipamentos serão reutilizados na proposta de reestruturação de rede. No entanto, alguns *Access Points* de baixa qualidade ainda precisarão ser substituídos conforme a tabela 9.

Tabela 9 : Equipamentos retirados na EBB Maria Garcia Pessi

Equipamento	**Modelo**	**Local**
Access Point Multilaser	Re171	Sala. Professores
Access Point Intelbras	WRN240	1ºAndar, lado direito
Access Point Intelbras	Win240	Sala 22

Fonte: Elaborada pelos autores.

A estrutura dessa instituição, é a maior entre as quatro escolas pesquisadas, nela será necessário adicionar vários equipamentos para suprir a necessidade de distribuição de wireless em toda escola. Os equipamentos que serão adicionados estão na tabela 10.

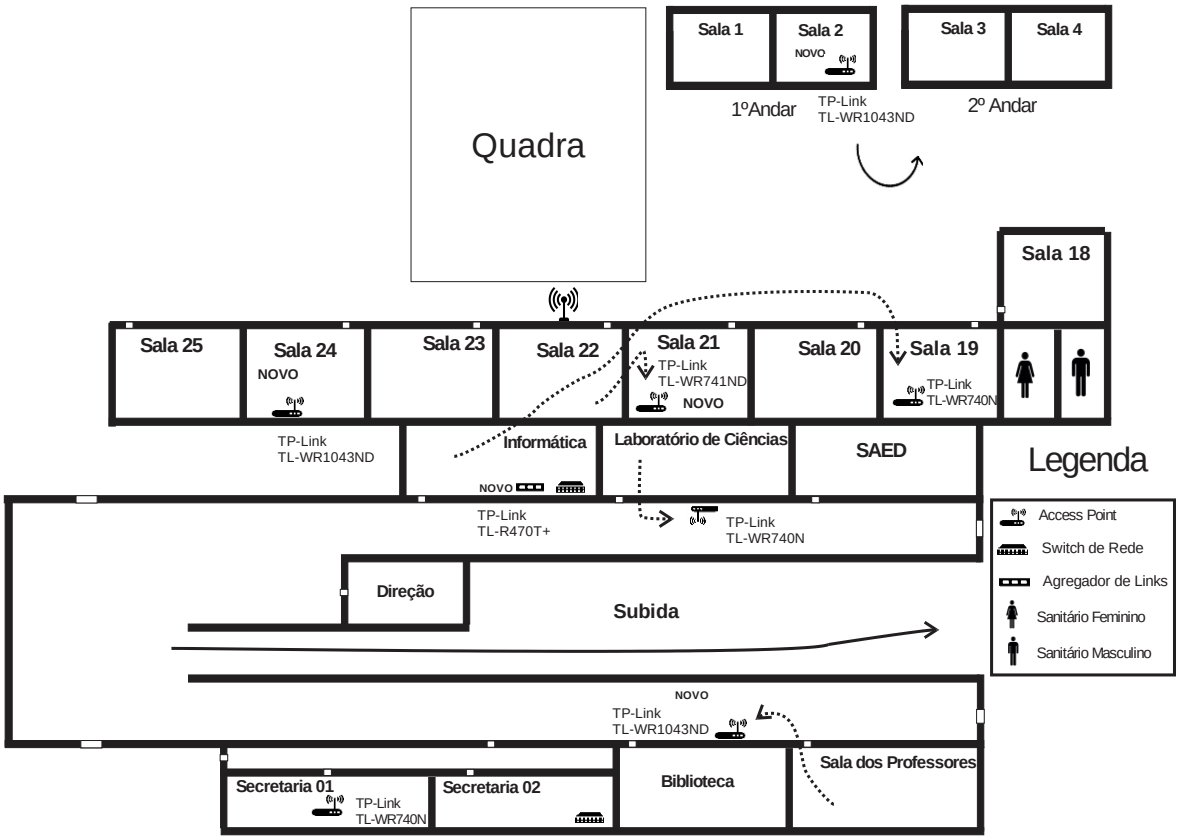
Tabela 10: Equipamentos adicionados na EBB Maria Garcia Pessi

Equipamento	**Modelo**	**Local**
Access Point TP-Link	TL-WR1043ND	Biblioteca, corredor
Access Point TP-Link	TL-WR1043ND	Sala 24
Access Point TP-Link	TL-WR741ND	Sala 21
Access Point TP-Link	TL-WR1043ND	Prédio, sala 02
Access Point TP-Link	TL-WR1043ND	1º andar, corredor esquerdo
Access Point TP-Link	TL-WR1043ND	2º andar, corredor direito
Roteador Balanceamento de Carga TP-Link	TL-R470P+	Informática

Fonte: Elaborada pelos autores.

Esses equipamentos terão sua distribuição ao longo do mapa escolar conforme as Figuras 17, 18 e 19.

Figura 17: Proposta para o térreo da EBB Maria Garcia Pessi



Fonte: Elaborada pelos autores.

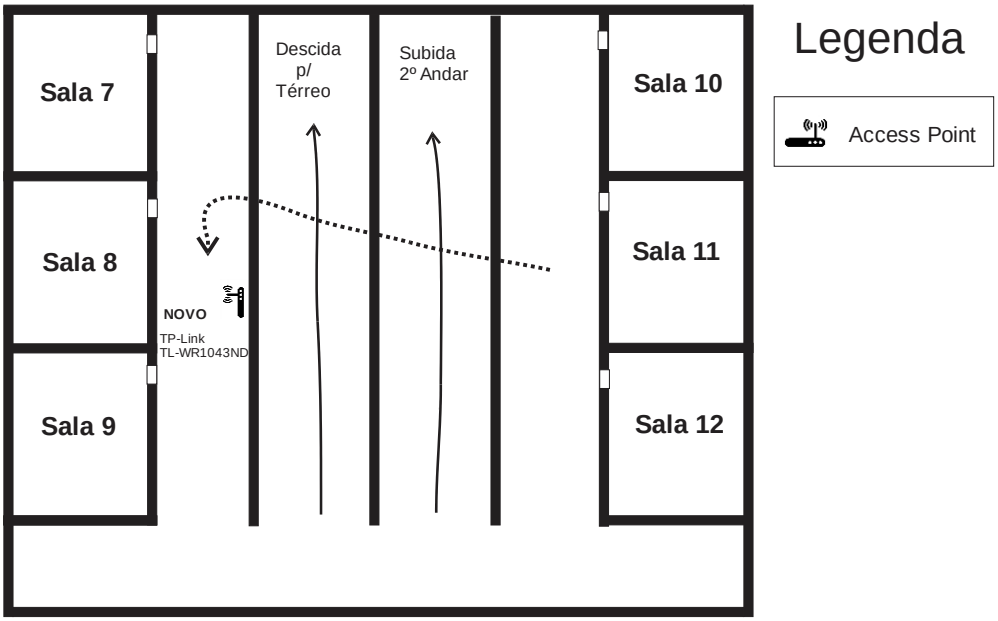
Embora o corredor da biblioteca disponha de sinal satisfatório, será necessário substituir o *Access Point* da sala dos professores e adicionar outro aparelho colocando-o no corredor, pois é necessário que todos os *Access Points* suportem o OPENWRT ou DD-WRT para existir um gerenciamento de senhas integrado e eficiente. Com essa mudança de local, o *Access Point* distribuirá melhor o sinal *wireless* no local, adicionando alcance suficiente para o lado direito do 1º andar.

Na estrutura atual da escola, existe um *Access Point* na informática e outro no laboratório de ciências, salas que ficam uma ao lado da outra, desperdiçando o sinal de wireless para a sala SAED ao lado. Para resolução desse problema, foi modificado de local o *Access Point* do laboratório de ciências, colocando-o no corredor em frente

a mesma. No laboratório de informática será reutilizado o *Access Point* TP-Link modelo TL-WR740N e movendo-o para a sala 19 acrescentando o alcance de sinal para as salas 18, 19 e 20. Nesse mesmo corredor serão adicionados dois novos *Access Points*, um TP-Link modelo TL0WR1043ND na sala 24, distribuindo sinal para sala 23, 24 e 25 e um TP-Link modelo TL-WR741ND na sala 21, que distribuirá sinal para as salas 21 e 22 e enviará sinal para a antena responsável pela propagação de sinal para o prédio logo a frente, salas 01, 02, 03 e 04, essa antena situa-se no telhado em cima da sala 22.

A última modificação necessária no térreo será a adição de um *Access Point* no prédio em frente, na sala 02. Esse *Access Point* será utilizado como um repetidor, replicando sinal *wireless* da antena para as salas 01, 02, 03 e 04.

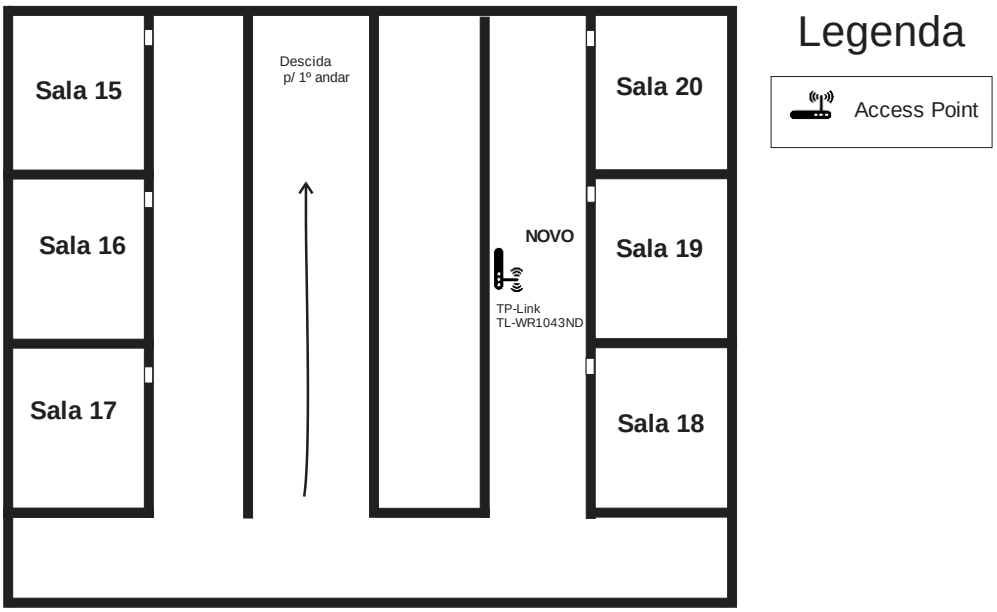
Figura 18: Proposta para o 1º Andar da EEB Maria Garcia Pessi



Fonte: Elaborada pelos autores.

No 1º andar, será feita uma substituição do *Access Point* Intelbras modelo WRN240 e deslocamento para o lado esquerdo do 1º andar, o lado direito terá o alcance de sinal do térreo onde foi adicionado o *Access Point* no corredor em frente a biblioteca.

Figura 19: Proposta para o 2º Andar da EEB Maria Garcia Pessi



Fonte: Elaborada pelos autores.

Já no 2º andar será adicionado um novo *Access Point* TP-Link modelo TL-WR1043ND no lado direito, distribuindo sinal para as salas 18, 19 e 20, pois planeja-se que o lado esquerdo consiga captar o sinal do *Access Point* adicionado à esquerda no 1º andar.

4.4 EEB DE ARARANGUÁ

A escola EEB de Araranguá dentre as quatro, é a que possui a melhor estrutura de rede, desse modo não é necessário adicionar *Access Points* padrão, somente um roteador de balanceamento de carga na sala de direção, para fazer o gerenciamento do link de 15MB/s atual da escola junto com o novo link de 15MB/s que será disponibilizado. As informações do roteador está detalhado na tabela 11.

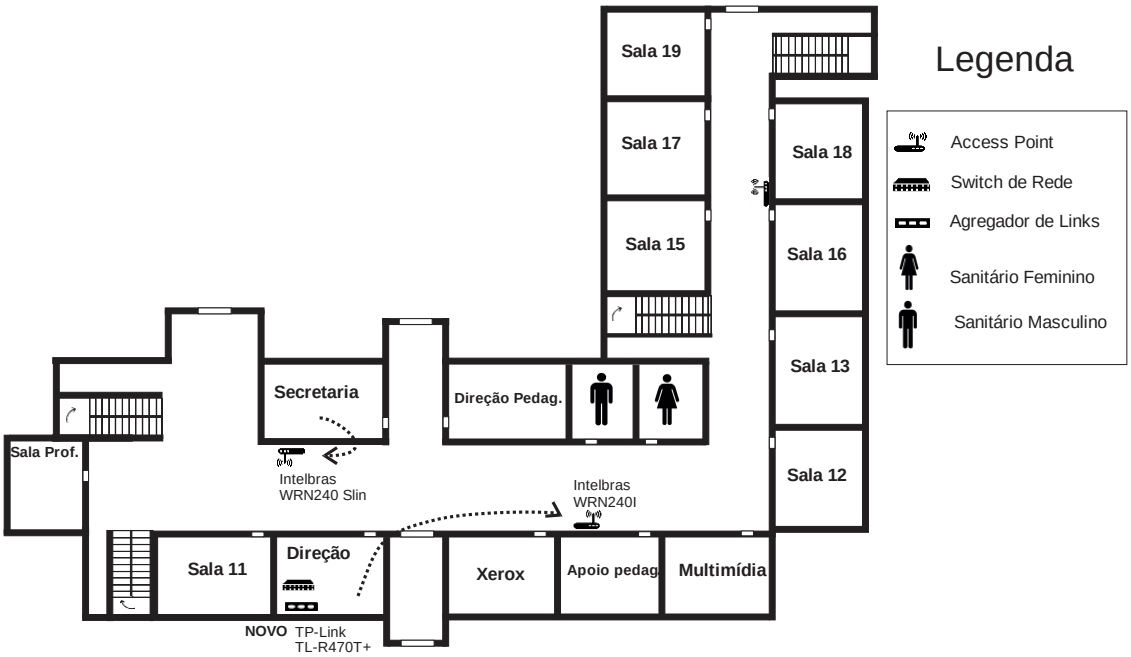
Tabela 11: Equipamentos adicionados na EBB de Araranguá

Equipamento	**Modelo**	**Local**
Roteador Balanceamento de Carga TP-Link	TL-R470P+	Direção

Fonte: Elaborada pelos autores.

O mapa da escola com a nova proposta de roteamento está detalhado nas Figuras 20 e 21.

Figura 20: Proposta para o térreo da EEB de Araranguá

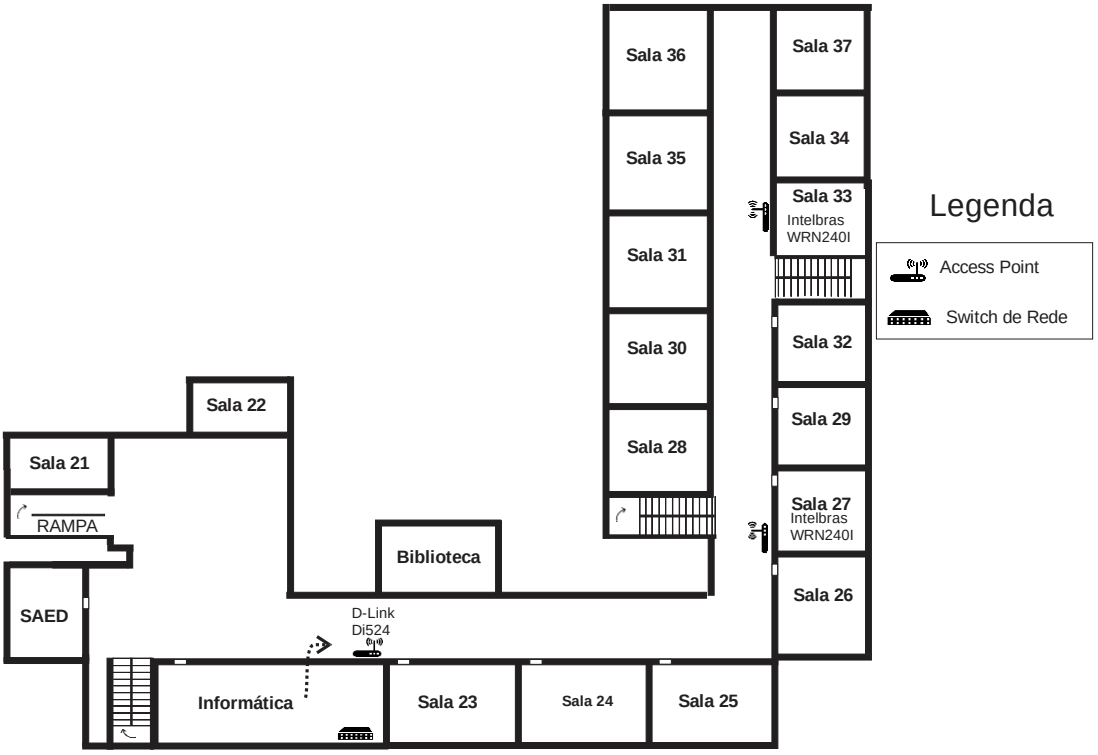


Fonte: Elaborada pelos autores.

Ainda que a escola possua uma ótima distribuição de sinal wireless, ocorre a possibilidade de melhorá-la conforme planejado na figura 20 e 21.

As salas apoio pedagógico e multimídia são as únicas salas que possuem um baixo sinal de wireless, desta forma, o *Access Point* Intelbras modelo WR240I da direção será movido para o corredor em frente a sala de apoio pedagógico e o *Access Point* da secretaria será colocado no corredor em frente a mesma, distribuindo melhor o sinal de wireless.

Figura 21: Proposta para o 1º andar da EEB de Araranguá



Fonte: Elaborada pelos autores.

No 1º andar da escola, a única modificação necessária será mover o *Access Point* D-LINK modelo DI524 de dentro da sala de informática para o corredor, adicionando cabeamento direto da sala de direção e deixando o link de 2MB/s para os computadores da sala de informática. Desse modo, o *Access Point* fará uma distribuição eficiente para as regiões que possuem baixo sinal de wireless como salas 21, 22, 23 e biblioteca.

4.5 EEB PROFº OTÁVIO MANOEL ANASTÁCIO

A escola EEB Profº Otávio Manoel Anastácio (OMA) possui atualmente três roteadores. O de melhor qualidade é utilizado como modem/roteador e os outros dois de de baixa qualidade, estão na sala dos professores e biblioteca, sendo necessário a substituição de todos, conforme a tabela 12.

Tabela 12: Equipamentos retirados EEB Profº Otávio Manoel Anastácio

Equipamento	**Modelo**	**Local**
Access Point TP-Link	TD-8816	Secretaria
Access Point Kaiomy	APR-4PN	Sala.Professores
Access Point Knup	Knup-kp-R02	Biblioteca

Fonte: Elaborada pelos autores.

Por ter uma estrutura pequena e os novos roteadores possuírem um longo alcance de sinal wireless, somente será necessário a inserção de dois roteadores wireless, um em frente a sala 12 e outro em frente à sala 05. Será também inserido um roteador de balanceamento de carga na sala 08 que fará a junção do link de 8MB/s existente na escola junto com o link de 15MB/s que será adicionado e distribuindo para os dois novos roteadores Tp-Link modelo TL-WR1043ND.

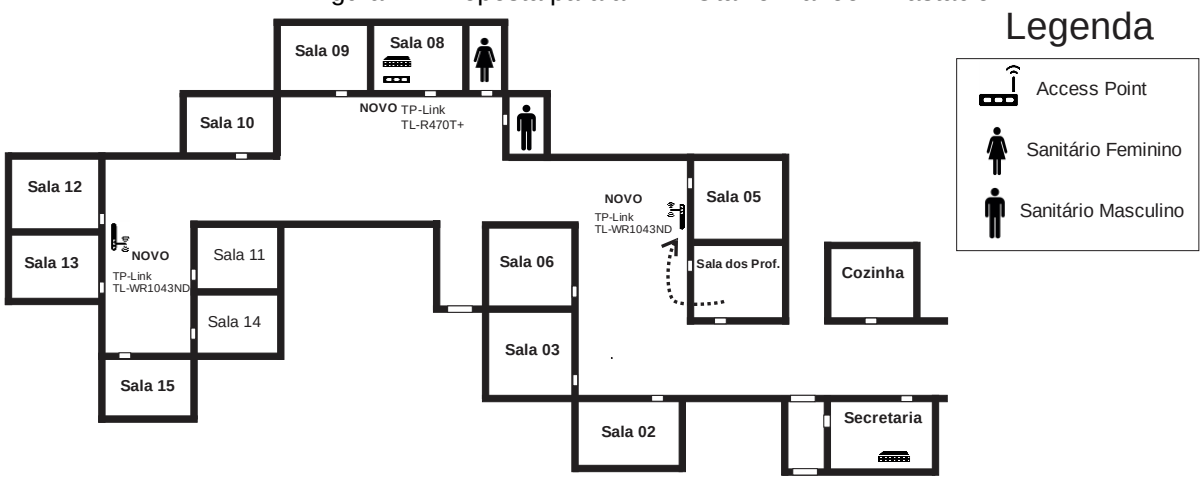
Tabela 13: Equipamentos adicionados na EEB profº Otávio Manoel Anastácio

Equipamento	**Modelo**	**Local**
Access Point TP-Link	TL-WR1043ND	Corredor, sala 12
Access Point TP-Link	TL-WR1043ND	Corredor, sala 05
Roteador Balanceamento de Carga TP-Link	TL-R470P+	Sala 08

Fonte: Elaborada pelos autores.

Proposta para a estrutura de rede da escola EEB Profº Otávio Manoel Anastácio :

Figura 22: Proposta para a EEB Otávio Manoel Anastácio



Fonte: Elaborada pelos autores.

A EEB Otávio Manoel Anastácio possui problemas de acesso a wireless principalmente no lado esquerdo da escola. As salas 09 à 15, ou possuem baixo sinal ou não possuem sinal algum. A estrutura atual mantém um *Access Point* na sala 02 que faz a divisão do link da CIASC da secretaria, de apenas 2MB/s, ou seja, a escola possui um *Access Point* na secretaria e outro *Access Point* na sala 02 fazendo uso do *link* CIASC. Como proposta, foi removido o *Access Point* da sala 02 e o *Access Point* da secretaria, deixando o *link* do CIASC exclusivamente para os computadores da secretaria. Desse modo, os links adicionados no roteador de balanceamento estarão distribuídos para os dois *Access Points* adicionados na escola. O *Access Point* Kaiomy modelo APR-4PN será substituído por um *Access Point* TP-Link modelo TL-WR1043ND e movido para o corredor em frente à sala 05, distribuindo sinal para as salas dessa região, enquanto outro *Access Point* será adicionado entre as salas 12 e 13, acrescentando um bom sinal wireless no lado esquerdo que atualmente é quase inexistente.

4.6 PROPOSTA DE SEGURANÇA DE REDES E GERENCIAMENTO DE SENHAS

Atualmente as escolas incluídas neste trabalho contam com um gerenciamento de senhas muito falho. Todas as escolas possuem problemas no gerenciamento das senhas dos *Access Points* e em alguns casos, os professores não conhecem a senha e não tem a quem recorrer caso haja algum problema em relação ao desempenho da

rede por sobrecarregamento após vazamentos de senhas. Então algumas escolas contratam empresas para fazer por exemplo uma troca de senha e isso leva tempo e dinheiro.

Para um gerenciamento simples e eficiente da rede sem fio, é necessário pensar em uma proposta em que não exija uma pessoa para fazer esse gerenciamento, já que as escolas não possuem um profissional capacitado. Pensando nisso, optou-se em utilizar os equipamentos da TP-Link que suportem os sistemas embarcados OPENWRT ou DD-WRT, na qual serão adicionado um script constado no apêndice A. Esse script é responsável pela geração e alteração de uma senha diária, reiniciando o *Access Point* principal e propagando a alteração para os outros *Access Points,* enviando um e-mail para cada conta externa e informando a nova senha. Para obter a nova senha, os professores devem acessar o e-mail através do link de internet da CIASC que ficará reservado apenas para os computadores da secretaria. Essa é a solução proposta para as escolas EEB Profº Otávio Manoel Anastácio, EBB Profª Maria Garcia Pessi e EEB Profº Apolônio Ireno Cardoso**.**

Para o caso da escola EEB de Araranguá, deve ser utilizado um servidor *raspberry pi,* implementando contas estáticas para os professores em um servidor *RADIUS,* pois os professores utilizam da rede sem fio para fazer a chamada dos alunos *online*. Para os alunos, o servidor criará uma conta de uso diário que utilizará um *script* com objetivo de trocar a senha como no caso das escolas citadas anteriormente. Desse modo, cada *Access Point* será configurado para buscar senha nesse servidor *RADIUS*.

Para a proteção de rede da escola, todos os *Access Points* utilizarão o protocolo de segurança WPA2 com chave criptografia AES proporcionando uma rede confiável e segura para as instituições.

5 CONCLUSÕES E CONSIDERAÇÕES FINAIS

Neste trabalho apresenta-se a viabilização de modificações na rede sem fio na estrutura de redes em quatro escolas, duas da rede estadual, escola Educação Básica Profª. Maria Garcia Pessi (Araranguá- SC) e Escola de Educação Básica Profº Apolônio Ireno Cardoso (Balneário Arroio do Silva - SC) e duas da rede municipal, Escola de Educação Básica de Araranguá e Escola de Educação Básica Profº. Otávio Manoel Anastácio, ambas em Araranguá. Possibilitando que os docentes durante a aula possam utilizar de práticas de experimentação remota.

Conforme pode ser visto no capítulo 1, foi aplicada uma pesquisa bibliográfica para dar o embasamento teórico necessário para o conhecimento de redes sem fio utilizado nas visitas e na proposta de reestruturação.

Um aspecto importante é que a prática nos auxiliou igualmente na criação do conhecimento, prática essa, adquirida principalmente nas diversas idas às escolas para a coleta de dados. As visitas foram importantes para que o aprendizado visto em disciplinas anteriores dentro da universidade fosse centralizado em um ponto específico, o uso de redes sem fio.

Com os dados coletados, iniciou-se o desenvolvimento de plantas baixas das escolas. Com as plantas podem ser encontradas as localizações exatas dos equipamentos disponíveis nas escolas. As plantas baixas foram utilizadas como forma de expor antes e depois dos locais, possibilitando ao leitor, uma forma prática de visualizar todo o trabalho feito.

Com a estrutura das escolas desenhada em mãos, captamos todos os novos equipamentos que serão utilizados no projeto e assim, desenvolvemos uma proposta que se encaixe nas necessidades. As propostas elaboradas, tiveram um foco principal de suprir as falhas encontradas na estrutura de wireless de rede nas instituições pesquisadas, além de proporcionar um eficiente gerenciamento de senhas utilizando poderosos protocolos de segurança de rede.

Como resultados, podemos afirmar que a reestruturação das escolas, é totalmente viável e pode ser executado, tendo em vista a melhora da distribuição da internet nas salas, um gerenciamento de senhas confiável e eficiente, além de uma

melhora na segurança dessas senhas, possibilitando assim, o uso pleno a tecnologia remota em sala de aula como foi apresentado no capítulo 4.

Portanto conclui-se que as escolas necessitam da mudança estrutural para que possam prover um ambiente apto a utilização da experimentação remota. A reestruturação da redes pode prover as escolas a possibilidade de novas atividades com o uso da tecnologia. Tablets, celulares e notebooks, podem contribuir nesse novo ambiente criado, fazendo com que a falta de um laboratório físico seja mero detalhe.

Inicialmente seriam aplicadas as mudanças nas quatro escolas, entretanto, devido a problemas burocráticos (atraso da licitação de equipamentos) tornou-se inviável a execução da proposta de melhoria. Portanto, este trabalho de conclusão de curso, mostra um caminho para aqueles que desejam modificar as escolas de uma forma efetiva, ao utilizar de duas maneiras distintas aplicadas de acordo com a necessidade atual das escolas.

A implantação que ocorreria, acabou por ser tornar uma proposta, devido ao limite de tempo atingido. Porém como um trabalho futuro, pode-se aplicar a proposta criada neste trabalho de conclusão de curso, abrindo o caminho para tecnologia dentro da sala de aula e assim deixamos uma sugestão para que sejam realizados novos estudos a respeito do tema futuramente.

REFERÊNCIAS

ABOBA, B. et al. **Extensible Authentication Protocol (EAP).** 2004. Disponível em: <https://www.ietf.org/rfc/rfc3748.txt>. Acesso em: 05 jun. 2017.

ABOUT DD-WRT. Disponível em: <http://www.dd-wrt.com/site/content/about>. Acesso em: 20 jun. 2017.

ANTUNES, Vítor Hugo Leite. **Frontend Web 2.0 para Gestão de RADIUS.** 2009. 84 f. Dissertação (Mestrado) - Curso de Engenharia Electrotécnica e de Computadores, Universidade do Porto, Desconhecido, 2009. Disponível em: <https://repositorio-aberto.up.pt/bitstream/10216/59427/1/000135708.pdf>. Acesso em: 20 maio 2017

ARTHAS, Kael. Tutorial Wireless. 2010. Disponível em: https://kaelnetworks.wordpress.com/2010/07/12/tutorial-redes-wireless/ . Acessado em: 12/04/2017

BARROS, Luiz Gustavo; FOLTRAN JUNIOR, Dierone César. **Autenticação IEEE 802.1x em Redes de Computadores Utilizando TLS e EAP.** 2008. Disponível em: <http://www.4eetcg.uepg.br/oral/62_1.pdf>. Acesso em: 20 maio 2017.

CAMARGO, Leandro de Lima; CORSINI, Fábio dos Santos. **REDES WIRELESS INDOOR E OUTDOOR.** 2010. Disponível em: <https://jornada.ifsuldeminas.edu.br/index.php/jcmch2/jcmch2/paper/viewFile/1722/1202>. Acesso em: 11 abr. 2017.

CHAVES, Tiago Rodrigues. **ESTUDO DE CASO: AUTENTICAÇÃO IEEE 802.1X BASEADA NO PROTOCOLO RADIUS E SERVIÇO DE DIRETÓRIO LDAP APLICADO A REDE GIGAUFOPNET.** 2010. 110 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Presidente Antonio Carlos - Unipac, Ouro Preto, 2010. Disponível em: <http://www.decom.ufop.br/imobilis/wp-content/uploads/2012/06/BCC391-102-vf-04.1.4174-TiagoRodriguesChaves.pdf>. Acesso em: 20 maio 2017.

DERMATINI, Felipe. **WEP, WPA, WPA2: o que as siglas significam para o seu WiFi?** 2013. Disponível em: <https://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>. Acesso em: 11 abr. 2017.

DUARTE, Carlos Anderson Andrade. **A EVOLUÇÃO DOS PROTOCOLOS DE SEGURANÇA DAS REDES SEM FIO: DO WEP AO WPA2 PASSANDO PELO WPA.** 2010. 51 f. TCC (Graduação) - Curso de PÓs-graduaÇÃo Lato Sensu em Redes de Computadores, Escola Superior Aberta do Brasil – Esab, Vila Velha, 2010. Disponível em: <https://www.esab.edu.br/wp-content/uploads/monografias/carlos-anderson-andrade-duarte.pdf>. Acesso em: 17 abr. 2017.

ENGST, Adam; FLEISHMAN, Glenn. Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh. 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005

FREIRE, Patrícia de Sá. **Aumente a Qualidade e Quantidade de Suas Publicações Científicas: Manual para elaboração de projetos e artigos científicos**. Curitiba: Crv (2013).

GAST, Matthew S.. **802.11 Wireless Networks:** The Definitive Guide. 2. ed. Sebastopol: Mike Loukides, 2005. 656 p.

GIOVANE DE MORAIS, 2016, Rio de Janeiro. **Segurança da Informação Através de Autenticação Centralizada por IEEE 802 1x Baseada em Protocolo RADIUS e Base de Dados LDAP Aplicada à Redes Sem Fio.** Rio de Janeiro: Aedb, 2016. 12 p. Disponível em: <http://www.aedb.br/seget/arquivos/artigos16/3024238.pdf>. Acesso em: 05 jun. 2017.

GIMENES, Eder Coral. **SEGURANÇA DE REDES WIRELESS.** 2005. 58 f. TCC (Graduação) - Curso de Faculdade de Tecnologia, Centro de Educação Tecnológica Paula Souza Faculdade de Tecnologia de Mauá, Muá, 2005. Disponível em: <http://www.tvprudente.com.br/apostilas/Rede/Redes.pdf>. Acesso em: 10 abr. 2017.

GODOY, A. S**. Introdução à pesquisa qualitativa e suas possibilidades**. In: Revista de Administração de Empresas. São Paulo: v.35, n.2, p. 57-63.

GONSALVES, E. P. **Escolhendo o percurso metodológico**. In: GONSALVES, E. P. Conversas sobre iniciação à pesquisa cientifica. Campinas: Alí- nea, 2001. p. 61-73.

GUISS, Alexandre. **O que é um Endereço MAC e como fazer para descobri-lo no seu computador ou smartphone.** 2010. Disponível em: <https://www.tecmundo.com.br/5483-o-que-e-um-endereco-mac-e-como-fazer-para-descobri-lo-no-seu-computador-ou-smartphone.htm>. Acesso em: 22 set. 2010.

HECK, Carine et al. **EXPERIENÊNCIA DE INTEGRAÇÃO DA EXPERIMENTAÇÃO REMOTA NO ENSINO DE FÍSICA DO ENSINO MÉDIO:** PERCEPÇÃO DOS ALUNOS. 2017. Disponível em: <http://seer.ufrgs.br/index.php/renote/article/view/70662/40099>. Acesso em: 18 jun. 2017.

HEERDT, Mauri Luiz; LEONEL, Vilson. **Metodologia Científica e da Pesquisa.** Palhoça: Unisulvirtual, 2007.

HOLMES, Thiago. **DD-WRT – Melhore e potencialize seu roteador.** 2016. Disponível em: <https://linuxcentro.com.br/linux/tutoriais/dd-wrt-melhore-e-potencialize-seu-roteador/>. Acesso em: 20 jun. 2017.

INTEL. **Visão geral e os tipos de EAP do 802.1.** 28 jan. 2017. Disponível em: <http://www.intel.com.br/content/www/br/pt/support/network-and-i-o/wireless-networking/000006999.html>. Acesso em: 20 maio 2017.

KAMEYAMA, Alexander. Estudo da tecnologia de acesso Wi-Fie suas aplicações em ambientes indoor e outdoor. 2013. 153 f. Trabalho de conclusão de curso (bacharelado - Engenharia Elétrica) - Universidade Estadual Paulista, Faculdade de Engenharia de Guaratinguetá, 2013. Disponível em: <http://hdl.handle.net/11449/119502>

KÖCHE, José Carlos. Fundamentos de metodologia científica: teoria da ciência e prática da pesquisa. 14. ed. rev. e ampl. Petrópolis: Vozes, 1997

KUROSE, James F.; ROSS, Keith W.. Redes de Computadores e a Internet: Uma Abordagem Top - Down. 5. ed. São Paulo: Pearson, 2010. 576 p.
LARROSA, Otávio Augusto G. et al. A influência e importância da criptografia na velocidade de redes Ethernet. 2013. Disponível em: <http://ftp.unipar.br/~seinpar/2013/artigos/Otavio Augusto Goncalves Larrosa.pdf>.

MENEGOTTO, Francisco Antônio. Expansão de rede Gigabit Ethernet. 2011. 58 f. TCC (Graduação) - Curso de EspecializaÇÃo em TeleinformÁtica e Redes de Computadores, Universidade TecnolÓgica Federal do ParanÁ, Curitiba, 2011. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/654/1/CT_TELEINFO_XIX_2011_10.pdf>. Acesso em: 10 abr. 2017.

MICROSOFT. Visão geral do PEAP. Disponível em: <https://technet.microsoft.com/pt-br/library/cc754179(v=ws.11).aspx>. Acesso em: 10 maio 2017.

MORIMOTO, Carlos e. Redes wireless, parte 2: Padrões. 2008. Disponível em: <http://www.hardware.com.br/tutoriais/padroes-wireless/pagina8.html>. Acesso em: 18 abr. 2017.

NICKEL, Eduardo Maltauro; BESSA, William Kuhl Svoboda Marques. **SISTEMA EMBARCADO COM ACESSO SEM-FIO.** 2010. 54 f. Monografia (Especialização) - Curso de Engenharia Elétrica, Universidade Federal do Paraná, Curitiba, 2010. Disponível em: <http://www.eletrica.ufpr.br/arquivostccs/158.pdf>. Acesso em: 20 jun. 2017.

Ohrtman, F.; Roeder, K. Wi-Fi Handbook: Building 802.11b Wireless Networks, 1a ed., McGraw-Hill, 2003.

OLIVEIRA, Alysson Nishiyama de. **AUTENTICAÇÃO EM REDES WIRELESS COM CERTIFICAÇÃO DIGITAL EVITANDO "EVIL TWIN".** 2007. 103 f. TCC (Graduação) - Curso de Engenharia de ComputaÇÃo, Centro UniversitÁrio de BrasÍlia – Uniceub, Brasília, 2007. Disponível em: <http://repositorio.uniceub.br/bitstream/123456789/3179/2/9965560.pdf>. Acesso em: 05 jun. 2017.

OpenWRT. OpenWrt Wiki - OpenWrt Wiki. Disponível em: . Acesso em: 19 de Junho de 2017

PAIM, Rodrigo R.. **WEP, WPA e EAP.** 2011. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/eap.html>. Acesso em: 27 maio 2017.

REDE Wireless DD-WRT: Guia Prático do Usuário Iniciante. Guia Prático do Usuário Iniciante. 2011. Disponível em: <http://jf.eti.br/wp-content/uploads/ddwrt-guiainiciante.pdf>. Acesso em: 20 jun. 2017.

ROCHADEL, Willian et al. ENSINO A DISTÂNCIA NA EDUCAÇÃO BÁSICA: a integração pedagógica de jogos digitais em ambientes virtuais. **E-tech: Tecnologias para Competitividade Industrial,** Florianópolis, v. 1, n. 9, p.32-54, jul. 2016. Disponível em: <http://revista.ctai.senai.br/index.php/edicao01/article/view/824/427>. Acesso em: 18 jun. 2017.

RUBINSTEIN, Marcelo G.; REZENDE, José F. Qualidade de serviço em redes 802.11. XX Simpósio Brasileiro de Redes de Computadores (SBRC2002), 2002.

RUFINO, Nelson Murilo de Oliveira. **Seguranças em Redes sem Fio:** Aprenda a proteger suas informações em ambientes wi-fi e bluetooth. 2. ed. São Paulo: Novatec, 2007. 206 p.

SANKAR, Krishna et al. **Cisco Wireless Lan Security:** Expert guidance for securing your 802.11 networks. Indianapolis: Cisco Press, 2004. 456 p.

SANTOS, Matheus Lincoln Borges dos. **Rede Mesh Wifi para disponibilização de acesso à internet.** 2011. 55 f. TCC (Graduação) - Curso de Engenharia Elétrica, Pontifícia Universidade Católica do Paraná, Curitiba, 2011. Disponível em: <http://www.pucpr.br/arquivosUpload/5370721951437430125.pdf>. Acesso em: 20 jun. 2017.

SIFURO, Sérgio Henrique. **ANÁLISE DE DESEMPENHO DE REDES IEEE 802.11B UTILIZANDO MECANISMOS DE SEGURANÇA.** 2005. 162 f. Dissertação (Mestrado) - Curso de Pósgraduação em Engenharia Elétrica, Departamento de

Engenharia Elétrica da Puc-rio, PontifÍcia Universidade CatÓlica do Rio de Janeiro - Puc-rio, Rio de Janeiro, 2005. Cap. 3. Disponível em: <https://www.maxwell.vrac.puc-rio.br/acessoConteudo.php?nrseqoco=21805>. Acesso em: 17 abr. 2017.Acesso em: 13 maio 2017.

SILVA, Juarez Bento da. **A UTILIZAÇÃO DA EXPERIMENTAÇÃO REMOTA COMO SUPORTE PARA AMBIENTES COLABORATIVOS DE APRENDIZAGEM.** 2006. 196 f. Tese (Doutorado) - Curso de Pós-graduação em Engenharia de Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis, 2007. Disponível em: <http://btd.egc.ufsc.br/wp-content/uploads/2010/06/Juarez-Bento-da-Silva.pdf>. Acesso em: 15 jun. 2017.

SILVA, Juarez Bento da; FISCHER, Benedito René; ALVES, João Bosco da Mota. Experimentação Remota em Santa Catarina. 2010. Disponível em: <https://periodicos.ifsc.edu.br/index.php/rtc/article/view/213>. Acesso em: 19 maio 2017.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. Metodologia da pesquisa e elaboração de dissertação. 3. ed. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001.

SIMAO, José Pedro Schardosim et al. Utilização de Experimentação Remota Móvel no Ensino Médio. Renote - Revista Novas Tecnologias na Educação, Porto Alegre, v. 11, n. 1, jul. 2013. Disponível em: <http://seer.ufrgs.br/index.php/renote/article/view/41701/26452>. Acesso em: 20 maio 2017.

STALLINGS, William; BROWN, Lawrie. Segurança de Computadores: Princípios e Práticas. 2. ed. Rio de Janeiro: Elsevier, 2014. 724 p.

SUPPORTED Devices. Disponível em: <http://www.dd-wrt.com/wiki/index.php/Supported_Devices>. Acesso em: 20 jun. 2017.

TANENBAUM, Andrew S.. **Redes de Computadores.** 4. ed. Rio de Janeiro: Elsevier, 2003. 955 p.

WPA: A evolução do WEP. Disponível em: <http://www.lockabit.coppe.ufrj.br/artigo/wpa-evolucao-do-wep>. Acesso em: 17 abr. 2017.

7 APÊNDICE – *SCRIPT* PARA O OPENWRT

```
#!/bin/bash

### INSTRUCOES ###
### E necessario gerar um par de chaves criptograficas RSA no AP
principal (ssh-keygen -t rsa) ###
### e distribuir a chave publica para os demais APs (scp
/root/.ssh/id_rsa.pub IP_AP:/root/.ssh/authorized_keys) ###
### E necessario instalar o pacote mutt (opkg update; opkg install
mutt) e configura-lo em /root/.muttrc ###
### alterando os seguintes parametros: "set from", "set spoolfile",
"set certificate_file", "set smtp_url" e "set smtp_pass" ###

### endereco de email destino ###
EMAIL=fulano@dominio.com.br
### lista de enderecos IP de cada AP ###
LISTA_AP="IP1 IP2 IP3"
### Gera uma senha aleatoria de 10 caracteres ###
SENHA=`< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c${1:-10};echo;`

### Altera a senha wifi do AP local e aplica a alteracao ###
uci set wireless.@radio0.key=$SENHA
uci commit wireless; wifi

### Altera a senha wifi dos APs remotos e aplica a alteracao ###
for i in $LISTA_AP
do
  ssh $i 'uci set wireless.@radio0.key=$SENHA'
  ssh $i 'uci commit wireless; wifi'
done

### Envia email com nova senha para o endereco cadastrado ###
mutt -F /root/.muttrc -s "Nova senha da rede WIFI" $EMAIL < $SENHA
```